AN ASSESSMENT OF THE IMPLICATIONS OF
‘HACKTIVISM’ FOR INTERNATIONAL RELATIONS

BY

SMITH ODURO-MARFO

(10307481)

THIS DISSERTATION IS SUBMITTED TO THE
UNIVERSITY OF GHANA, LEGON, IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE
AWARD OF THE MASTER OF ARTS DEGREE IN
INTERNATIONAL AFFAIRS

LEGON

JULY 2015
DECLARATION

I hereby declare that this work is entirely my research except the references that have been made to the works of other authors. Such references have been cited and duly acknowledged. I assume full responsibility for this work.

ODORO-MARFO SMITH
(STUDENT)

DR. BONI YAO GEBE
(SUPERVISOR)

DATE: ...........................  DATE: ...........................
DEDICATION

I dedicate this work to God, my mother, Ama Gyamfuaa and my two wonderful sisters, Elaine and Anita for being there for me through thick and thin.
ACKNOWLEDGEMENT

I will like to acknowledge the efforts of my supervisor, Dr. Boni Yao Gebe for his insightful guidance of this work. I reserve special gratitude for Dr. Philip Attuquayefio and Dr. Linda Darkwa for their unconditional support throughout my MA studies. I am also grateful for the support of Dr. Peace Medie, Mrs. Afua Yakohene, Ms. Rita Boateng and members of the 2015 LECLIAD class particularly Nana Ekua Awotwi, Staniel Ayikwei, Dieu-Donne Gameli, Owusua Kankam, Glenn Norgbey, Ebenezer Anderson, and Zaharau Shariff. To the ‘Ardays’ especially Charlotte, I am colossally thankful. I acknowledge the support of my great friends; Vincent Asante Asiedu, Kwadwo Opoku Danso, Obed Afrane, Michael Yekple, Beatrice Brew, and Kwabena Mensah.
## LIST OF ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AQAP</td>
<td>Al-Qaeda in the Arabian Peninsula</td>
</tr>
<tr>
<td>cDc</td>
<td>Cult of the Dead Cow</td>
</tr>
<tr>
<td>CNN</td>
<td>Cable News Network</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DRIPA</td>
<td>Data Retention and Investigatory Powers Act</td>
</tr>
<tr>
<td>ECJ</td>
<td>European Court of Justice</td>
</tr>
<tr>
<td>EDT</td>
<td>Electronic Disturbance Theatre</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EZLN</td>
<td>Zapatista National Liberation Front</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>IR</td>
<td>International Relations</td>
</tr>
<tr>
<td>ISC</td>
<td>Intelligence and Security Committee</td>
</tr>
<tr>
<td>ISIS</td>
<td>Islamic State in Iraq and Syria</td>
</tr>
<tr>
<td>NAFTA</td>
<td>North American Free Trade Agreement</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>US (A)</td>
<td>United States (of America)</td>
</tr>
<tr>
<td>WANK</td>
<td>Worm Against Nuclear Killers</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>
## Table of Contents

DECLARATION ................................................................................................................. i  
DEDICATION .................................................................................................................... ii  
ACKNOWLEDGEMENT ................................................................................................. iii  
LIST OF ACRONYMS ..................................................................................................... iv  
ABSTRACT ...................................................................................................................... vii  
CHAPTER ONE ................................................................................................................. 1  
  Research Design.............................................................................................................. 1  
  1.1 Background to Research Problem ............................................................................. 1  
  1.2 Statement of the Research Problem .......................................................................... 3  
  1.3 Research Questions ................................................................................................... 4  
  1.4 Objectives ................................................................................................................. 4  
  1.5 Rationale of the Study ............................................................................................... 4  
  1.6 Scope of the Study .................................................................................................... 4  
  1.7 Hypothesis................................................................................................................. 5  
  1.8 Theoretical Framework ............................................................................................ 5  
  1.9 Literature Review...................................................................................................... 9  
    1.9.1 Hacktivism and Hacking; do they share a common ethic? .............................. 9  
    1.9.2 Hacktivism and the Law ................................................................................. 11  
    1.9.3 Hacktivism and Diplomacy ............................................................................. 13  
    1.9.4 Developing a Theoretical Framework for Hacktivism .................................... 15  
  1.10 Sources of Data ..................................................................................................... 18  
  1.11 Research Methodology ......................................................................................... 18  
  1.12 Arrangement of Chapters ...................................................................................... 19  
Endnotes............................................................................................................................ 20  
CHAPTER TWO .............................................................................................................. 22  
  Overview of Hacktivism and its History ...................................................................... 22  
  2.1 Defining Hacktivism ............................................................................................... 22  
    2.1.1 What is Hacking? ............................................................................................ 22  
    2.1.2 What is Activism? .......................................................................................... 24  
    2.1.3 What is Hacktivism? ....................................................................................... 26  
  2.2 History of Hacktivism ............................................................................................ 27
4.3 Recommendations..................................................................................................... 78
Endnotes........................................................................................................................... 80
BIBLIOGRAPHY ............................................................................................................. 81
ABSTRACT

Hacktivism generally refers to the use of computer hacking to pursue socio-political change. The budding academic literature on hacktivism has paid more attention to its usage as a tool of protest and its legality. This work thus focuses on the practical implications of hacktivism for international security and inter-state relations. To do this, the study guided by the theory of Pluralism specifically assesses the implications of the hacktivist activities of Anonymous, WikiLeaks and Edward Snowden. The study concludes that hacktivism has generally had positive implications for international security. However, in terms of inter-state relations, hacktivism has generally had negative implications due to the major tensions that it has fostered in the bilateral relations of some states. The study recommends that states utilise the evidence in the information revealed by hacktivists to reassess and improve their foreign relations. States can also collaborate with hacktivists in the cyber-based aspects of the fight against terrorism. Also, it is recommended that future academic works should pursue the interpretation of hacktivism in the context of other states to balance the America-centric nature of the literature on hacktivism.
CHAPTER ONE

Research Design

1.1 Background to Research Problem

‘Hacktivism’ is a coinage from two words; ‘hack’ and ‘activism’. Hacking is the act of using a computer to gain an unauthorized access to another computer to breach its data or to manipulate its functions.¹ Activism generally involves a person or a group noticing a problem in society and taking action to address the problem with the aim of creating change.² Hacktivism thus basically refers to “a marriage of political activism and computer hacking”.³ Some of the notable names that have come to be associated with hacktivism include WikiLeaks, Anonymous, Cult of the Dead Cow (cDc), Electronic Disturbance Theatre (EDT) and individuals like Julian Assange, Edward Snowden and Bradley Manning among others.

Hacktivists are a class of non-state and often, transnational actors. A major tactic of hacktivists has been to reveal classified information of entities including states.⁴ In the case of states, the leaks are supposedly to hold governments accountable and transparent but also to promote good causes such as human rights.

In April, 2010, WikiLeaks for instance, published a classified video which showed American soldiers launching unprovoked air strikes leading to the death of 12 civilians in Iraq.⁵ That same year, WikiLeaks published tens of thousands of damaging official documents on America’s war in Afghanistan and Iraq.⁶ In 2011, Anonymous played a
significant role in supporting the Arab Spring particularly in Tunisia and Egypt. In June 2013, Edward Snowden leaked numerous confidential files of the National Security Agency (NSA) exposing how the American state had been spying on its citizens and even foreign leaders like the German Chancellor, Angela Merkel.

While America has charged Snowden with stealing classified government information, Russia has granted Snowden temporary asylum. Austria broke diplomatic protocol to search the presidential plane of Bolivia due to the suspicion that Snowden was on board. While Britain is ready to extradite Julian Assange to face trial in Sweden, Ecuador has harboured Assange in its embassy in London after granting him political asylum.

In the early 2000s, the Electronic Disturbance Theatre, a pioneer hacktivist organization rendered practical support to help Mexico’s indigenous Zapatista Movement in fighting for their rights. This and other instances like Anonymous’ help to protesters during the post-election stand-off in Iran in 2009 and during the 2011 Arab Spring plus the emergence of African hacktivist groups like Anonymous Africa (Zimbabwe), Naija Cyber Hacktivists (Nigeria) and GhostShell (South Africa) point to the fact that hacktivism is not only targeted at governments of developed countries nor a first world phenomenon but genuinely a growing global concern.

In the minds of international relations students and practitioners, these happenings are likely to suggest a complex - for according to the realists, non-state actors are insignificant actors in the international system who do not influence significantly
international relations. However, the fact that hacktivists leak to the public what states do not want the public to know and proceed to pressurise states (and even at times pressurise non-state actors) in the name of pursuing socio-political change likely holds significant ramifications for international security and inter-state relations.

1.2 Statement of the Research Problem

Hacktivists by their non-state and often transnational nature, can due to internet technology sit anywhere in the world and put pressure on any government to demand transparency, accountability and protection of human rights among others. Hacktivism thus immediately presents a challenge for states. States are increasingly facing political activism that is pursued not only by residents within the state but immensely aided by several faceless internet users across the world.

Again, hacktivists in the name of promoting global public interest go to the extent of accessing classified state information and leaking them into the public domain. This deepens the challenge posed by hacktivism to states. If the secret actions and intentions of a state are leaked, that state cannot be sure of the reactions of its citizens and the international community to the declassified information. While hacktivists claim that their activities promote global public interest, targeted states have often decried hacktivism as a danger to international security.

The hacktivist thus is a modern actor that potentially changes the dynamics of the international system and as such, is worthy of academic investigation. The budding literature on hacktivism has paid more attention to its usage as a tool of protest and the
legality of hacktivism. Though there are also academic works on the ramifications of hacktivism for diplomacy, they have mostly taken a predictive approach instead of assessing the actual impact on the ground. This research work used an evidence-based approach to study the implications of hacktivism for international relations, specifically in the contexts of international security and inter-state relations.

1.3 Research Questions

1. What is the history and nature of hacktivism?

2. How does hacktivism affect international security?

3. To what extent do hacktivists influence inter-state relations?

1.4 Objectives

1. To understand the nature and history of hacktivism.

2. To assess the implications of hacktivism for international security.

3. To assess the extent to which hacktivism affects inter-state relations.

1.5 Rationale of the Study

Hacktivism by its nature is likely to sustain its head-on collision with various governments around the world. Thus this study is important, as an understanding of the practical impact of hacktivism on international relations helps actors in world politics to tap into and improve the positive utility of hacktivism while minimising its negative effects. The work also helps contribute to the literature on hacktivism.

1.6 Scope of the Study

Due to the ever-growing number of hacktivists and the limited time for the completion of this work, this study focused mainly on the activities of WikiLeaks, Anonymous and
Edward Snowden that relate directly to governments. The three actors were selected due to the huge media coverage they have enjoyed and also due to their structural differences. WikiLeaks is a formal organization while Anonymous is not a formal body. Edward Snowden operated as an individual and belongs to no hacktivist group.

The study limits itself to the period from 2006 to June, 2015. This period is basically chosen because WikiLeaks and Anonymous were not founded before 2006 while Edward Snowden’s leak was in 2013. Regarding the implications of hacktivism for international relations, the study limits itself to discussions on the conduct of inter-state relations and international security. This study does not seek however to investigate the processes of hacking.

1.7 Hypothesis
Hacktivism has had positive implications for international security and inter-state relations.

1.8 Theoretical Framework
The theory that guided this study is pluralism. Pluralism was the second strongest theoretical challenge against realism after idealism. While idealism challenges realism’s assertion that the state and humans are of a nature that is irredeemably conflict-prone, pluralism sidesteps that debate to rather attack the state-centric focus of realism. Basically, pluralism posits that the state is not the only actor in the international system. To pluralists, there exist other significant non-state actors in the international system that must not be overlooked in international relations analysis. Pluralism as a theory of international relations emerged in the late 1960s and became popular from the 1970s. The
leading proponents of pluralism include but are not limited to Kal Holsti, Robert Keohane and Joseph Nye.

The flagship works espousing the tenets of pluralism are Transnational Relations and World Politics; and Power and Interdependence. Both books were written by Nye and Keohane. Nye and Keohane strongly explicated the main assumptions of pluralism each of which directly challenged widely-held realist assumptions which they deemed as inadequate. It must be said that before Keohane and Nye, other authors had earlier expressed the pluralist position in one way or the other. For example, Arnold Wolfers had earlier emphasized that an evolving international system had come to witness the emergence of a host of non-state entities that are “able on occasion to affect the course of international events” and thus become “actors in the international arena and competitors of the nation-state”.

The underlying assumptions of pluralism as intimated by Nye and Keohane and highlighted hereafter are founded on their assertion that the activities of the soldier and the diplomat that have become the most quintessential in the analysis of realists do not occur in a vacuum. Such activities are very much affected by geography, domestic politics and technology.

Resulting from this phenomenon is the first assumption of pluralism which is that the state is not the only significant actor in the international system as posited by realism. There are other actors that are trans-governmental and transnational in nature who
significantly affect international relations. To pluralists, there are sub-state actors that influence the activities of states thus the international system by providing inputs that may not necessarily be the same as that of the state. As such, the realists are wrong to say that the state is a unitary/coherent actor in foreign policy making. There also are transnational actors who exert significant influence in the international system like some multinational companies.

The second assumption according to Nye and Keohane is that international issues or foreign policy issues have no hierarchies. This again contradicts the realist position that issues of the military (war and peace) are always at the pinnacle on the state’s list of issues/priorities. They posit that the agenda for world politics has become extensive such that issues relating to the environment, economics and migration among others have also jumped to the forefront. To Nye and Keohane, the distinctions that exist between domestic and foreign policies have become blurred and the role of the non-state actor in the agenda-setting of states as a result has become more pronounced. Another assumption by the pluralists is that due to the emergence of new actors and new issues in international relations, there has come into existence a certain interdependence between actors in the international system such that resorting to military force to ensure the national interest is relegated to the background in many cases.

According to Nye and Keohane, the specific effects of non-state/transnational actors on inter-state politics include; increased constraints on states through dependence and interdependence, increased ability on the part of some governments to influence others
and the emergence of autonomous actors who promote foreign policies that may deliberately oppose or impinge on state policies. Generally, non-state actors “increase the sensitivity of societies to one another and thereby alter relationships between states”.

Pluralism has however been met with many criticisms. Some of these criticisms are highlighted hereafter.

An often-made accusation against pluralism as an international relations theory has been that it is not necessarily a unitary theory rather it is an assembly of theories. Joseph Grieco for example, in making this point points to the functional integration theory, neo-functional regional integration theory and the interdependence theory which all preceded pluralism but basically are of a common strand. Richard Little also criticizes that pluralism is western-oriented and that it has a disposition towards a liberal political order which is not necessarily existent in every country. Last but not least, a crucial criticism against pluralism has been levelled by structural realists like Kenneth Waltz. To the structural realists, the anarchy in the international system and the resulting security dilemma is time-tested and indispensable in international relations analysis and as such, scoff at pluralists for rejecting these concepts as a given.

Notwithstanding the criticisms against pluralism, it is relevant as a theory to guide this work primarily because the theory is hinged on the categorical assertion that non-state actors like states can also be significant actors in the international system and even affect how states behave. This study primarily is about hacktivists and the implications that their activities have for international relations. By definition, hacktivists are a class of
non-state actors of a transnational nature. Once this definition is accepted, then hacktivists and their activities challenge the realist position that states are the only significant actors in the international system and also that states are unitary actors. The realists’ virtual disregard for the role of non-state actors in the international system also suggests that non-state actors cannot impact a state’s national interest. Hacktivism questions the credentials of realism and backs the assertions of pluralism as shown in this study.

1.9 Literature Review

This section reviews some of the major academic works that have been done on hacktivism thus far. The review of the literature utilizes a thematic approach. The main themes are; hacktivism as a tool of protest, the legality of hacktivism, the impact of hacktivism on diplomacy and the development of a theoretical framework for hacktivism.

1.9.1 Hacktivism and Hacking; do they share a common ethic?

In ‘From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?’, Paul Taylor attempts to prove the existence of a common ethic between hacktivists and hackers.17 To do this, Taylor initially traces the history of hacking. He advances that there have been seven generations of hackers and that hacktivists form the seventh generation. According to Taylor, the first five generations of hackers had little to do with activism. These generations mainly hacked as an end in itself without the motivation of initiating or catalysing campaigns for socio-political change. The pre-occupation of these earlier generations is basically with how beautiful or difficult the hack is. On the other hand, the last two generations have had a lot to do with activism.
The sixth generation is tagged by Taylor as the “Open Source movement”. This generation, he explains is made up of hackers who believe that information should be free and accessible to all. This generation mainly safeguards the right to information and as such will do everything possible to ensure that information can be accessed by all with little or no hindrances. In this light, the sixth generation hacks into software programmes that can originally be accessed at a fee with the aim of making it free to all. By doing as such, the sixth generation actually had a social cause that it pursued. Thus hacktivism builds upon the goal of the sixth generation by mainstreaming direct political action as its main objective. Taylor indicates that unlike the preceding generations of hackers, hacktivists are not concerned about the beauty or difficulty of the hack but about how much of a political point it makes. The difficulty with Taylor’s categorization is that it makes it very challenging to describe ‘WikiLeaks’ for instance, as a hacktivist organization. This is due to the great emphasis on the ‘hack’ in ‘hacktivism’. WikiLeaks’ official position is that it only publishes leaks but does not hack itself into the databases of others for the information it leaks.

Taylor asserts that hacktivism is a return to the fundamental elements of the original ethics of hacking. The elements he points out are; using technology ingeniously, reverse-engineering technology so it does what it was not intended to do and the desire to test systems. To make this point, Taylor interestingly steps outside his seven hacking generations into Ancient Greece. He taps into an allusion that the earliest hacktivists can be said to have been the ‘Demos’ (the ordinary people) in the Agora. In Ancient Greece, the Agora was the centre for Logos (intellectual, rational and polite discourses on key
matters concerning the Polis). However, often the Demos interjected and disrupted the discourse using ‘Nomos’ (symbolic speech), which encompassed demonstrations and the making of unwelcome gestures. To Taylor, the Demos are akin to hacktivists, as they opposed the dominant rationality of the day.

This allusion quite stretches thin the definition of a hacktivist. Accepting the allusion will almost open the floodgates for many forms of popular protestations to qualify as hacktivism. For instance, the actions of the demos in the Agora are not markedly different from a group of citizens marching into the national legislative chamber or court to protest. Notwithstanding, Taylor does well to prove how hacktivism shares a common strand of ethics with original hacking despite the inter-generational differences when it comes to pursuing a social cause.

1.9.2 Hacktivism and the Law

In ‘Hacktivism: A New Breed of Protest in a Networked World’, Noah Hampson explores where hacktivism sits in relation to the law.18 Hampson quickly stresses that the legal regimes both at national and international levels are not really tailor-made to govern hacktivism. To mitigate the potential challenge that such a gap presents, Hampson advises that courts should first assess whether an act of hacktivism was pursued in a damaging manner or not. In this regard, he argues that hacktivist acts that merely serve an expressive function must not be grouped with all others and be deemed criminal in the face of the law. More specifically, Hampson presents that hacktivism which does not involve the hijacking of computers or networks and also does not cause any significant damage like virtual sit-ins must not be criminalized. Hampson buttresses this position by
alluding to non-virtual non-violent protest. According to him, some degree of damage resulting from hacktivism must be tolerated just as a degree of damage caused by peaceful physical protests is accepted.

The challenge with Hampson’s position however is that; it is difficult to compare the virtual and physical realms when dealing with the concepts of violence, peace and damage. Unlike in a street protest, it is difficult to determine which form of hacktivism can be said to be peaceful or which damage can be generally agreed upon as tolerable. Hampson’s main reason for arguing for hacktivism to attain some legality is that hacktivism has positives as it allows protesters to push for change despite their limited power, poverty, location or the oppression they are being put through especially by the government of the day. One of the earliest to write on the legality of hacking was Kenneth Himma. In ‘Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?’; Himma concludes that hacktivism cannot be harboured under the umbrella of the law insofar as it results in significant harm to third parties.\(^{19}\) Once again, the big question becomes what can be classified as ‘significant harm’ and who determines it; the hacktivist, the target or the law courts?

In “Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime”, Xiang Li contributes impressively to the discussion on hacktivism and the law.\(^{20}\) Li specifically attempts to assess the legality of hacktivism as an instrument of protest in the light of the First Amendment of the American Constitution. Li concludes that over time, hacktivism may evolve to fall under the ambit of the First Amendment but
will first have to circumvent certain primary and secondary barriers. The big primary barrier for Li is the coverage of the First Amendment. To Li, the First Amendment seeks to prevent a specific actor, ‘government’ from abridging freedom of speech in a specific context; ‘the public forum’. This according to Li suggests that where the target of hacktivism is not the government, invoking the First Amendment is difficult. Also, the answer to whether government-owned or privately-owned websites constitute public fora is unclear according to Li. Li posits that as things stand now, cyber-attacks that are via the creation of pop-up windows on a targeted website can arguably be protected under the First Amendment. A criticism against Li’s work is its almost total concentration on the kind of hacktivism which utilizes cyber-attacks. Li, like Hampson, believes that a total prohibition of all forms of hacktivism may greatly hinder the positive utilities of that form of protest.

1.9.3 Hacktivism and Diplomacy

WikiLeaks’ declassification of thousands of diplomatic cables (nicknamed ‘Cablegate’), in 2010 incited some academic commentary on the impact of hacktivism for diplomacy. For example, Robert Saunders’ ‘WikiLeaks are Not Terrorists–A Critical Assessment of the “Hacktivist” Challenge to the Diplomatic System’ does a good job in exploring the topic.\(^{21}\) Saunders’ central thesis is that WikiLeaks has not necessarily influenced the structure of diplomacy such that it has led to a change in how diplomacy is pursued. Saunders posits that the internet has endowed individuals and groups of individuals with a substantial amount of power. He even goes as far as to say that probably individuals due to the internet wield so much power in global politics like never before in world history.
Saunders proceeds to make an interesting comparison between Julian Assange and Leon Trotsky (of the former Soviet Union) on the basis that they both sought to influence how diplomacy is conducted. Trotsky as a diplomat-gone-rogue published the secret covenants of the Entente during World War I, similar in a way to Assange’s ‘cablegate’ over ninety years later. Saunders highlights the diplomatic status of Trotsky and indicates that there is a difference between Trotsky and Assange as the latter is not affiliated to any national government. Saunders indicates that the hegemonic conditions in 1917 required that only persons highly connected to state power could potentially ensure political change. However, Saunders posits that both Trotsky and Assange despite the enormity of their leaks did not succeed in altering the way states pursue diplomacy. Saunders concludes that it is expected that states affected by the leaks will openly castigate and brand Assange as a terrorist despite the negligible practical damage done to the structure of diplomacy by the revelations. From Saunders’ allusion to Leon Trotsky can be inferred the important point that the leaking of high level state secrets existed even before the emergence of the cyberspace and more especially, hacktivism.

Nicholas Cull has also delved into the discussions comparing Trotsky and Assange and their impact on the conduct of inter-state diplomacy. Unlike Saunders, Cull asserts that both leaks were game-changers. Trotsky’s publication of the covenants for instance, encouraged American President, Woodrow Wilson to include in his ‘Fourteen Points’ a promise to pursue a more transparent diplomacy. Regarding the leaks by WikiLeaks, Cull notes that it is an indication of how powerful the individual (as a non-state actor) has
become in world politics due to the internet and as such, highlights the need for governments around the world to embark more on public diplomacy.

Towing the line of Saunders, Mark Page and Spence Jack also insist that WikiLeaks’ ‘cablegate’ has not in any significant way affected the conduct of diplomacy across the world. To them, the revelations instead of attaining the goal of increased transparency will rather increase secrecy. They make the notable point that if Woodrow Wilson could not remove secrecy from inter-state diplomatic dealings, Julian Assange cannot. From the foregoing discussion in this sub-section, it can be deduced that the literature on hacktivism and diplomacy has largely been predictive and not necessarily based on evidence on the ground. This work helps to bridge that gap by assessing how hacktivism has practically affected inter-state relations.

1.9.4 Developing a Theoretical Framework for Hacktivism

Despite the abundance of theories in international relations, Wendy Wong and Peter Brown in ‘E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One’, argue that none of those theories explains the peculiar nature and activities of hacktivists adequately. To them, the hacktivist is a new kind of political actor that has caused a fundamental change in global activism. Wong and Brown posit that the best description for the hacktivist is ‘Extraordinary Bandit’ or ‘E-bandit’. To them, hacktivists are extraordinary for reasons such as; their ability to resist the people in authority who threaten internet freedom, their opposition to the use of lobby as a tool to influence legislators and their favourable disposition to access what has been deemed off-limits like
classified state information. Wong and Brown emphasize how technology has altered the nature of “ordinary” transnational activism such that it expands the space for participation and without leaving any physical traces, still has real-world effects.

The principal argument by Wong and Brown is that hacktivism needs a customized theory that provides a best-fit explanatory framework. They exhibit this necessity by indicating how hacktivists are different from terrorist organizations, non-governmental organizations, social movements and international criminal networks (ICNs) though they are all non-state actors. To them, terrorism is totally not comparable to hacktivism due to the fact that hacktivism due to its virtual nature cannot satisfy the operational definitions of terrorism in terms of resorting to violence, for instance. Regarding ICNs, the differences include the prominent intent of corrupting public officials on the ground which hacktivists do not engage in. However, NGOs and social movements are said to be close but not fully the same as hacktivists. Wong and Brown thus propose the theory of ‘Politics of No-one’. The theory largely is centred on the anonymity that comes with hacktivism. Hacktivists unlike the afore-mentioned groups, embark on massive campaigns yet conceal the identity of the campaigners.

In a critique of the theory of Politics of No-one, Charli Carpenter wonders whether there is actually the need for a new theory to describe hacktivism. To Carpenter, if pushed, the nature of hacktivism may be efficiently described by other theories using the same tenets of those theories but explaining them in a customized manner. Carpenter’s position
can be buttressed for instance by the fact that pluralism can generally explain hacktivism as hacktivists are non-state actors that are sub-state and often transnational.

As sub-state actors, hacktivists for instance prove the pluralist position that states are not unitary and coherent actors. As transnational actors, hacktivism also proves the pluralist position that states are not the only significant actors in the international system. Admittedly, the part that pluralism fails to explain is that hacktivists are largely anonymous. However, Carpenter rightly challenges the ‘hacktivism is about anonymity’ idea by indicating that Julian Assange for instance has not been anonymous. It is based on this logic that Carpenter describes the activities of Assange and WikiLeaks as “Politics of a very specific someone”. Notwithstanding, Wong and Brown have started an interesting conversation on whether a new theory is required to explain hacktivism or not.

The academic works reviewed in this section are part of the growing number of works on hacktivism. However, they reasonably represent the major discourses regarding hacktivism. The literature on hacktivism is budding and as such, understandably has many gaps. However, new literature on the subject is increasingly getting these gaps reasonably filled. For example, Leonie Maria Tanczer’s recent publication, ‘Hacktivism and the Male-only Stereotype’, introduces a refreshing gender perspective to the hacktivism discourse. Moving on, what this study has attempted to do is to help bridge the gap in the literature on hacktivism by paying more attention to the practical implications of hacktivism for inter-state relations and international security.
With regards to foreign relations, the often-cited work is Dorothy Denning’s ‘Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy’. However, this work was published in 1999, over half a decade before the emergence of major hacktivists like WikiLeaks, Anonymous and Edward Snowden. A lot has changed since 1999 thus it is necessary to take a new look at hacktivism and inter-state relations. Moreover, the recent works discussing hacktivism and diplomacy have mainly been predictive and have hardly used an evidence-based approach in reaching conclusions. Regarding the implications of hacktivism for international security, the discourse has largely been outside the academic domain and largely speculative. Thus it is imperative that a look is taken at the issue academically.

1.10 Sources of Data
The sources of data for this study were secondary in nature. These sources were mainly books, journal articles, news items (both in print and on the internet), published research works and government documents (like reports and press statements) relevant to the topic under discussion. Credible video documentaries and interviews useful to this study were also utilized.

1.11 Research Methodology
For this study, a qualitative methodology was used. With this, a case study approach was utilized as three specific hacktivists were studied in the context of the implications of their activities for international relations. These three actors; WikiLeaks, Anonymous and Edward Snowden were sampled purposively. Despite the existence of numerous hacktivists, these three hacktivists were deliberately chosen out of the lot particularly as a result of the huge media coverage they have enjoyed as well as the structural differences
between them. In a bid to investigate the stated problem of the study, document analysis was utilized, guided by the research questions and objectives. As such, the study critically reviewed and analysed information carried in books, academic journals, official documents and news items, among others, relevant to the topic of the study to deduce findings and draw conclusions.

1.12 Arrangement of Chapters

For this study, Chapter One presents the Research Design. Chapter Two details the nature and history of hacktivism. Chapter Three analyses the implications of hacktivism for International Relations while Chapter Four presents a summary of the findings and conclusions of the study. Additionally, the study also makes a number of recommendations in Chapter Four.
Endnotes

1 This is only a narrow definition as aside computers, hacking could also be other machines being made to function in a way that they are not originally supposed to. "Hack, n.1." *OED Online*. Oxford University Press, December 2014. Web. 1 January 2015.


4 Generally, hacktivism is different from cybercrime as the perpetrators of the former supposedly are motivated by a pursuit of an improvement in the welfare of society. However, this conception has always been dicey as a targeted individual or organization is likely to see hacktivism as criminal.


6 This according to WikiLeaks was the "most significant archive about the reality of war to have ever been released during the course of a war". WikiLeaks. https://www.wikileaks.org/afg/. July 25, 2010.

7 Incensed by the internet-censorship by the authoritarian regimes in the two countries, Anonymous supported the local protesters by attacking key government websites and also providing the protesters with software packages that helped to circumvent the internet censorship. McLaughlin, Victoria. *Anonymous: What do we have to Fear from Hacktivism, the Lulz, and the Hive Mind?*. Diss. University of Virginia, 2012.


13 See page 336. Ibid.


CHAPTER TWO

Overview of Hacktivism and its History

2.1 Defining Hacktivism

This chapter presents an overview of the nature of hacktivism and its history. This first sub-section seeks to define hacktivism. Hacktivism as a word is a neologism coined from hack and activism. Thus this researcher believes that an understanding of hacking and activism as independent activities will help provide a firmer footing for understanding what hacktivism is. As such, hacking and activism are explained after here, followed by a look at some definitions of hacktivism. Subsequently, the history and forms of hacktivism are discussed in this chapter.

2.1.1 What is Hacking?

The word ‘hack’ and its derivatives ‘hacker’ and ‘hacking’ generally evoke the thought of some young nerdy people who are obsessed with the computer and use the computer as a tool to pursue various forms of electronic illegalities. Concerning this picture of hacking, Taylor and Jordan have shown that it is erroneously taken for granted that hacking must be for perpetrating illegalities. Hackers are not generically cyber-criminals. Those who are deemed as using the computer to pursue illegalities are differently tagged as crackers in the hacking world, for instance. This position is admittedly debatable as what constitutes an illegality is not determined by the supposed perpetrators. Fundamentally, gaining unauthorized access to the computer system, machine or network of another entity is likely to sit on the wrong side of the law. Brian Harvey in his work, ‘What is a Hacker?’ discusses the legality or otherwise of hacking.
To Harvey, there is a difference between a hacker and a cybercriminal. He refers to the hacker as an “aesthete” and proceeds to indicate that

“Someone who sets out to crack the security of a system for financial gain is not a hacker at all. It’s not that a hacker can’t be a thief, but a hacker can’t be a professional thief. A hacker must be fundamentally an amateur, even though hackers can get paid for their expertise. A password hacker whose primary interest is in learning how the system works doesn't therefore necessarily refrain from stealing information or services, but someone whose primary interest is in stealing isn't a hacker. It's a matter of emphasis”.

Here, Harvey asserts rather controversially that the true hacker is innately ethical or moral or at the least, intending to disrupt but not to cause harm. However, the legality or otherwise of hacking is too subjective to be settled anytime soon, that is if the debate is being situated within the confines of motive. Else, gaining unauthorized access and tampering with the registered property of another entity are in themselves hardly legal.

The book, ‘Hackers, Heroes of the Computer Revolution’ authored by Stephen Levy discusses the ethic of hackers. In Levy’s words, it is one of “sharing, openness, decentralization, and getting your hands on machines at any cost to improve the machines and to improve the world”. Hackers basically see themselves as some geniuses primarily interested in getting a machine to work in such a manner that it was not originally designed to. Turkle describes the hacker as a “virtuoso programmer”. This ethic of hackers is better depicted in the story of the famous Homebrew Hacker Club. The club was made up of a number of hackers who dedicatedly shared knowledge and collaborated in a bid to improve the earliest form of the personal computer. Their efforts quickened the development of games, graphics and music among others as components of the computer. To do this, these hackers had to tamper with the products of others to know what they were made of and develop them further. By the time the club was no more, twenty three
computer companies had evolved from it.\textsuperscript{5} These companies included Apple. For the stated purpose of this work, the question of the legality of hacking is not of primary concern, hacking for socio-political change is. The brief effort however, is to indicate that hacking is not automatically a tool for illicit ends.\textsuperscript{6}

\textbf{2.1.2 What is Activism?}

“There are many varieties of activism, from the face-to-face conversations to massive protests, from principled behavior to the unscrupulous, from polite requests to objectionable interference, and from peaceful protests to violent attacks. Activism is not well defined, so different people often have somewhat different ideas of what constitutes activism. Activism is not necessarily a good thing or a bad thing. It all depends on the cause and the actions, and a person's judgment of what is worthwhile. One person might say that a protest is a valuable defense of freedom and another person might say that it is a dangerous attack on human rights.”\textsuperscript{7}

The above quotation is an attempt by Brian Martin to explain activism. Baumgardner and Richards have defined activism as “everyday acts of defiance”.\textsuperscript{8} Though, this definition represents what activism basically is, it may be too broad for academic purposes. This is because “everyday acts of defiance” can include and rightly so, too many actions including acts which may not be deemed by the actors as defiant though seen as such by a second party. Moreover, the definition looks at the action part of activism and ignores the issue of the intended function of the action. A more helpful definition thus is “action on behalf of a cause, action that goes beyond what is conventional or routine”\textsuperscript{.9} This immediately suggests that activism is ‘extraordinary’ defiance even where the action may look simple. Extraordinary as used here infers that activism pursues intended goals through sustained intended actions.

Activism becomes political when it seeks to bring a change in society.\textsuperscript{10} Such a change has been described as a “transgression”; pushing for societal structures to change from
things /arrangements that may have come to be accepted as normal.\textsuperscript{11} It must be said also that activism may seek to prevent a change in the status quo. In that sense, activism will be preserving what has come to be deemed as normal or traditional. For instance, when Abraham Lincoln, William Wilberforce and others campaigned for the abolition of slave trade, they were pursuing a ‘transgression’ from what had become deemed as normal. On another hand, there were Americans in the South who advocated for the maintenance of the status quo. Thus what makes an action one of activism is not at all that it is good or bad but that it is a sustained effort to cause a social change or in some cases, maintain the status quo.

Activists have over the years, pursued their goals through varying means. Some of the means are embarking on rallies and protest marches, embarking on educational campaigns, distributing leaflets, going nude on the streets, sending letters to various authorities and going on hunger strike, among others. The onset of the internet did open up a lot of channels that activists deployed to pursue their campaigns. One of the popular protest tools in recent times for instance, has been the collation of the signatures of petitioners on the internet. This digital tool ensures that many more people across the world get to hear about a campaign and get the opportunity to join no matter where they are. A number of websites are solely dedicated to supporting e-petitions for example. Clearly, the emergence of the internet has been of great benefit to activism and a key part of hacktivism.
2.1.3 What is Hacktivism?

“I've never thought there was a lot of debate about the meaning of hacktivism. It's a word that was coined by Omega - a longstanding member of the CULT OF THE DEAD COW (cDc) - in 1996. He used hacktivism to describe hacking for political purposes. Originally it was more of a quip or a joke. But from the first moment I heard Omega use it I knew that it would have profound meaning, not just for the cDc, but for millions of people across the Internet. Almost immediately "hacktivism" spread like wildfire. The word sounded so cool everyone wanted to use it - the trendier-than-thou digerati, on-line news editors, and especially washed-up activists who had just discovered email. Suddenly, everyone became a "hacktivist." No one had a clue what it meant, but it sounded cool.”

The above quote is by Oxblood Ruffin and provides a brief history of the origin of the word hacktivism. Evidently, the nature of the word lends itself to a generic definition. Hacktivism has generally thus been defined as the convergence of hacking and activism. For example, Jordan and Taylor define hacktivism as “a combination of grassroots political protest with computer hacking… activism gone electronic”. Dorothy Denning defines hacktivism as “the marriage of political activism and computer hacking”. Thus simply put, if hacking is utilized in activism then it is hacktivism. In other words, if a person or group of people centralizes hacking as a tool in the pursuit of ‘transgression’ in society, then it is hacktivism. Conceiving hacktivism in the light of Brian Martin’s definition of ‘activism’ will be; hacking “on behalf of a cause, action that goes beyond what is conventional or routine”.

The definition of hacktivism by Dorothy Denning helps to rope in the various shapes that hacktivism is taking and has taken over the years. According to Denning, “hacktivism is the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends”. This definition reduces the centrality of hacking to practical hacktivism and this ensures that other digital tools that facilitate and sustain the motive of hackers seeking to use their craft to promote socio-political change are duly recognized. Such digital tools
includes WikiLeaks’ safe drop-off online location which has solely been created to help hackers aiming to promote the public interest by revealing secret documents of various target parties from states to private corporations.

2.2 History of Hacktivism

Although the word ‘hacktivism’ was only coined in 1996, the first major use of hacking for socio-political purposes was recorded in 1989. Central to this act of hacktivism was the ‘Worm Against Nuclear Killers (WANK)’. WANK has been described as “the most famous worm in the history of computer networks” and also as the “first major worm bearing a political message”.

National Aeronautics and Space Administration (NASA) had planned to deploy a space shuttle carrying the Galileo Space Probe from Earth to Jupiter originally in October, 1989. The essence of the probe was to primarily study and investigate conditions on the planet Jupiter and its moons. The decision was to use nuclear energy to power the probe. Thus the energy demands of Galileo were to be met by a pair of radioisotope thermoelectric generators (RTGs). The RTGs were meant to generate electricity from the decay of plutonium 238 dioxide. Many anti-nuclear activists opposed this decision. These activists protested and some even took the matter to the court. Anti-nuclear activists argued that if the nuclear-bearing Galileo unfortunately exploded like its predecessor, the Challenger did, it would be disastrous for the environment and humanity.
On October 16, 1989, two days before the deployment of the probe into space, NASA computers were attacked by a computer worm.\textsuperscript{22} It is “a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code”.\textsuperscript{23} The computer networks of other agencies including the Fermi National Accelerator Laboratory, a nuclear facility near Chicago belonging to the US Department of Energy were affected. Also the European Organization for Nuclear Research based in Meyrin, Switzerland and the Riken Accelerator Facility in Japan had their computers affected. The worm posted unusual messages on the computer screens of these agencies.

The most notable message was the one below:

\begin{center}
\textbf{WORMS AGAINST NUCLEAR KILLERS}
\textbf{WANK}
\end{center}

\begin{center}
Your System Has Been Officially WANKed
\end{center}

\begin{center}
You talk of times of peace for all, and then prepare for war.
\end{center}

Source: Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier.\textsuperscript{24}

There was a second WANK attack within a few days. Though these agencies were eventually able to fend off the attack, they could not find the perpetrator(s). What was clear however was the political goal of the attack; the attack was a protest against the use of nuclear energy to power the Galileo probe and also a possible attempt to derail the lift-off by disrupting the computer systems. This motive was made clearer due to the
realization that the programmer of the worm had instructed it not to attack computers in New Zealand, a nuclear-free zone. New Zealand had in 1986 supported the anti-nuclear campaign strongly by barring America from entering New Zealand ports with ships bearing nuclear arms or powered by nuclear energy.  

The next major use of hacking to pursue socio-political change came in 1998 when the Electronic Disturbance Theatre (EDT) used the cyberspace as an avenue to support the Zapatista Movement. The Zapatista Movement is broadly a group of indigenous Mexicans that opposed capitalist globalization in their country. The group was mainly based in Chiapas, Mexico and was organized around the Zapatista National Liberation Front (EZLN). The movement’s practical goal was to place pressure on the Mexican government to ensure that the indigenous Mexican gains access to “work, land, housing, food, healthcare, education, independence, freedom, democracy, justice, and peace”.  

The signing of the North American Free Trade Agreement (NAFTA) in 1992 by America, Canada and Mexico has been noted as having significantly incensed the movement. On January 1, 1994 the EZLN led a rebellion in San Cristobal de las Casas, Chiapas and sustained the challenge to the Mexican government thereafter. From 1994, the movement used the internet to make a clarion call for people and groups around the world to support their cause. This clarion call was heeded by the Electronic Disturbance Theatre in 1998 after the Acteal Massacre.
The EDT aided the Zapatista Movement by developing the FloodNet software.\textsuperscript{30} FloodNet was designed to help replicate physical sit-in protests on the internet. With the software, many online protesters can visit the same website and cause the website to not function properly by automatically reloading the page over a considerable amount of time. FloodNet aids online protesters to make repeated requests to a specific website simultaneously thus causing that website to be overloaded with traffic such that it goes offline or goes down, at least for a while. This is called a Denial of Service (DOS) attack.

The Electronic Disturbance Theatre convinced many internet users around the world to join the struggle of the Zapatista Movement. With the FloodNet software, online sympathizers of the Zapatista Movement joined hands to bring attention to the plight of indigenous Mexicans by attacking the websites of the then Mexican President, Ernesto Zedillo; the then US President, Bill Clinton and the Mexican Stock Exchange among others.\textsuperscript{31} Clearly, the EDT had used hacking to pursue political change and by developing the FloodNet software had taken hacktivism to another level.

In 1999, hacktivism gained more attention due to how the internet was used to challenge the World Trade Organization (WTO) during its conference in Seattle. The online protest was engineered by a group called the Electrohippies Collective or ehippies. The protest has been described as “the most obvious and emblematic ever undertaken” in terms of online direct actions.\textsuperscript{32} The WTO faced intense opposition from mass protesters in Seattle in 1999.\textsuperscript{33} These protesters opposed the exploitation of developing countries by developed countries and mega corporate entities in the name of international trade. To the protesters, the supposed rules of international trade promoted by organizations
particularly the WTO unfairly marginalized and deepened the economic woes of poor countries and advantaged developed countries and their big multinational corporations.\textsuperscript{34}

The Electrohippies Collective took the mass protest online. The aim of the group was similar to that of the protesters marching on the streets; the disruption of the WTO meeting. The ehippies masterminded and promoted a denial of service attack against the website of WTO and other websites necessary for the running of the Seattle meeting. To do this, the ehippies designed a software programme and posted on their website with an accompanying explanation that the WTO was the target of the software. Anybody who went ahead to download the software saw his/her computer sending multiple requests to bombard the WTO network.

According to the ehippies, about 450,000 people or at least different computers participated in the protest attacks over a 5-day period.\textsuperscript{35} As later recorded by the ehippies; on 30\textsuperscript{th} November and 1st December, 1999 the servers of the WTO were interrupted.\textsuperscript{36} The WTO servers also slowed down significantly on the 2\textsuperscript{nd} and 3\textsuperscript{rd} of December, 1999 thus disrupting the Seattle meeting to some extent.\textsuperscript{37} The Electrohippies Collective fronted a follow-up protest attack against the computer networks of the International Monetary Fund and the World Bank in 2000 in Prague.\textsuperscript{38} This second protest only led to the intermittent slowdown of the targeted computer networks and involved about 5000 protesters.
The preceding paragraphs do not imply that the three incidents were the only ones concerning hacktivism nor that the engineers of these hacktivist initiatives were the only ones in the decade highlighted. However, they are some of the major incidents in the history of hacktivism. In more recent times, hacktivism has gained more prominence. The three hacktivist actors that this study looks at; WikiLeaks, Anonymous and Edward Snowden have richly contributed to the evolving history of hacktivism. Their hacktivism has cut across issues and countries; the details and impact of which will be discussed in the next chapter.

2.3 Forms of Hacktivism

The sub-section discusses the forms of hacktivism. With forms of hacktivism, what is being referred to is the modus operandi - how hacktivists practically pursue their quest for socio-political change. The forms of hacktivism discussed hereafter are guided by the work of Alexandra Samuel.\textsuperscript{39}

Denial of Service (DOS) attack: This refers to intentionally increasing the traffic to a specific website such that the website becomes too overloaded to operate. Often times, DOS attacks end up slowing the targeted website/ computer network or even taking it offline. Such a heavy traffic is artificially generated with automated software.

Information theft: This refers to hacking into a computer network and copying the information that is stored on it. On many occasions, hacktivists publish such information in the public domain.
Software development: This can be a form of hacktivism in which software is intentionally developed for political purposes. Such software is often open source (free) and allows internet users to bypass internet restrictions imposed by governments. An example is the TOR browser which allows internet users to browse the internet without leaving any discernible traces.

Website defacement: This refers to hacking into a web server and replacing a web page with another web page. Normally, the new page replacing the original one is used by hacktivist to present a specific message criticizing the targeted organization.

Website redirect: This refers to hacking into a web server and changing its web address such that internet users to the site end up visiting a different website. Normally, this different website carries a message often critical of the targeted organization.

Website parodies: With this, the hacktivists create a spoof website with a Uniform Resource Locator (URL) address that is close to that of the targeted organization’s website. As such, it is likely that the two web addresses will be confused by internet users and as such, many internet users will end up on the paroding website. The spoof website created by the hacktivists will often carry a message criticizing the targeted organization.

Virtual sabotage: Here, the intention of the hacker is to sabotage the computer networks of the targeted organization. To do this, the hacktivist infects the computer network with a worm or a virus as in the case of the WANK attack.
Virtual sit-ins: With this, traffic to a targeted website is intentionally generated by getting many internet users to visit a particular website at a particular time. This slows the website and depending on the number of participants who choose to partake and keep reloading the pages of the targeted website, the website can temporarily become inaccessible.

2.4 The Hacktivism of WikiLeaks, Anonymous and Edward Snowden

2.4.1 WikiLeaks

WikiLeaks which was officially launched in 2007 (though it began work in 2006) and sees itself as a media organization is dedicated to publishing hitherto undisclosed information made available by anonymous sources. Its main objective is to promote transparency and accountability around the world. Julian Assange is the lead-founder and the face of WikiLeaks. The official position of the organization is that it does not solicit information but only provides a safe environment for whistle-blowers to drop off the crucial information they have. WikiLeaks has designed and rolled out a highly encrypted website where whistle-blowers can safely submit information.

In that light, WikiLeaks posits that it does not hack into the computer systems of entities for information. The organization bases its activities on the 1946 United Nations Declaration of Human Rights particularly Article 19. The organization provides further legitimacy to its activities by making references to a US Supreme Court Ruling on Daniel Ellsberg’s leak of the Pentagon Papers during the Vietnam War. In that case, the court ruled that "only a free and unrestrained press can effectively expose deception in
government”. WikiLeaks has since 2007 published several major stories and official documents in the sphere of politics, commerce, warfare, human rights and diplomacy among others.

The biggest revelations published by WikiLeaks are mainly official documents on America’s conduct of its war in Afghanistan (Afghan War Diary), America’s conduct of its war in Iraq (Iraq War Logs) and diplomatic cables involving several members of the American Foreign Service across the world (Cablegate). The leaked diplomatic cables had information about several countries bordering on national security and even the personal information about some world leaders. WikiLeaks also in a major way exposed a $3 billion corruption in the Daniel Arap Moi presidency in Kenya and also the excessive maltreatment of inmates by American soldiers in Guantanamo Bay prison. The Afghan War Diary which was published in July, 2010 had 76,900 different files while the Iraqi War Logs published in October, 2010 had about 400,000 files. The Cablegate also had about 250,000 leaked cables. However, not all of these documents have been published.

2.4.2 Anonymous

Unlike WikiLeaks, Anonymous cannot be described as an organization with a known organogram and a known leadership. At best, Anonymous can be described as a movement of to a large extent, faceless hackers located at different places across the world. Unlike WikiLeaks, Anonymous hacks into the computer systems of its targets. These hackers generally do not know each other in real life and are only connected by
their common presence on internet chat rooms. One of such chat rooms that have been integral to the evolution of Anonymous is 4chan.

4chan is a website which basically is for chatting. Users of the website more often than not engage in trolling.\(^42\) The first time that these members engaged in an online activity that came close to hacktivism was in January 2008 in what they called Project Chanology. Project Chanology was in response to an ultimatum by the Church of Scientology to Youtube for a video featuring Tom Cruise (the famous Hollywood actor) to be taken offline.\(^43\) The Church of Scientology had also threatened all other websites that had hosted the Tom Cruise video with legal action.\(^44\)

Users on 4Chan opposed this ultimatum and collaborated online anonymously in a virtual opposition to the Church of Scientology.\(^45\) The group began by significantly boosting the presence of the video on the internet. Also, they engineered denial of service (DOS) attacks against the Church’s website and even campaigned against the human rights record of the Church among others. Project Chanology seems to have given these hackers a bit of a direction as to how they can use their skill to pursue political action. In 2010, the group also embarked on ‘Operation Avenge Assange’. This operation was meant as a virtual attack against Visa, MasterCard and PayPal.\(^46\) These companies succumbed to the pressure of the US government and blocked donations to WikiLeaks which were being sent through their payment systems.\(^47\) Anonymous thus directed massive DOS attacks against the websites of these commercial entities.
Subsequently, Anonymous has embarked on several operations (normally tagged as AnonOps). These include supporting protesters in Iran in 2009, Arab Spring protesters in 2011 and the Occupy Movement. Several government websites have been attacked by Anonymous including those of US, Uganda, Israel, Egypt and Tunisia among others. Recently, Anonymous has pursued an online war on the fundamentalist group, Islamic State in Iraq and Syria (ISIS). The Anonymous brand has grown across the world such that there are a number of Anonymous franchises globally. The group is symbolized by the Guy Fawkes mask.

2.4.3 Edward Snowden

In May, 2004 Edward Snowden enlisted as a trainee in the American army but was later discharged. Snowden’s superior programming skills landed him a job with the Criminal Investigations Agency (CIA) in the middle of 2006. In 2007, the CIA posted Snowden to Geneva as a telecommunications information systems officer. His task was to secure the computer systems of the CIA and American diplomats. Snowden resigned from the CIA in February, 2009 and was contracted by Dell Computers to work at an NSA facility in Japan.

In 2012, Snowden was posted to the regional cryptological centre of the NSA in Hawaii and his work primarily was to spy for the American state on foreign interests. In 2013, Snowden moved to work with Booz Allen Hamilton, one of the giant private security contractors in America. Snowden was contracted as a systems administrator and had a top-secret clearance. This level of clearance allowed Snowden access to a massive list of computer systems that had been hacked by the NSA. A few months into his work at Booz
Allen Hamilton, Snowden leaked thousands of classified top-security files from the internal servers of the NSA and GCHQ. The leaks were principally released through three newspapers; Guardian (UK), New York Times (US) and Der Spiegel (Germany). Snowden personally elicited the help of the journalist Glen Greenwald and film-maker Laura Poitras (two people who have been closely watched by the US government due to their sustained criticisms of America) in publishing the sensitive documents.

The leaks constituted a huge exposé on major undercover activities of the NSA in particular. The highlight of the leaks was the NSA’s very expansive surveillance programme. As part of the programme, America was spying on about 35 heads of state (including Angela Merkel, the Chancellor of a country seen as an ally of America) and collecting records of the electronic communication of people in America and beyond including that of Americans. The Snowden leaks also revealed the Five Eye partnership. This was a security intelligence-sharing partnership between US, Britain, New Zealand, Australia and Canada. These countries were spying on people in their region and sharing it in the name of counter-terrorism. On why he engineered the leaks of such sensitive documents, Snowden indicates that;

"Much of what I saw in Geneva really disillusioned me about how my government functions and what its impact is in the world. I realised that I was part of something that was doing far more harm than good…"\(^5^0\)

"…They [American government] are intent on making every conversation and every form of behaviour in the world known to them…”\(^5^1\)

2.5 Conclusion

This chapter has presented a general overview of hacktivism and its history. Before the definition of hacktivism was discussed, the chapter first explored the meaning of the two
key components that constitute hacktivism; hacking and activism. The point was made that hacking, historically, is not computer-centric and also not conceived generically as a vice by some hackers. The closing sections of the chapter presented the history and forms of hacktivism. The next chapter presents the implications of hacktivism for international relations in terms of international security and inter-state relations.
Endnotes


5 The documentary by Discovery Channel, “The Secret History of Hacking” provides great insight into the genesis of mainstream hacking. See [https://www.youtube.com/watch?v=Y47m1cOyKjA](https://www.youtube.com/watch?v=Y47m1cOyKjA).

6 Ibid.


11 Ibid.


14 Denning, Dorothy E. ’’Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy.’’ *Networks and Netwars: The future of Terror, Crime, and Militancy* 239 (2001): 288.


16 Op. Cit. See Denning, Dorothy E.


As one newspaper described at the time, Galileo was “the most sophisticated interplanetary probe ever built” and “promises to revolutionize knowledge about the solar system’s largest planet during an unprecedented 20-month orbital tour that will begin six years after the launch from Atlantis”. Atlantis was the name of the space shuttle from which the Galileo probe would launch. See *NASA gears up for Galileo Flight*. Lodi News Sentinel. p9. Retrieved from [https://news.google.com/newspapers?id=2245&date=19890814&id=FYQzAAAAIAJ&sjid=yzIHAIAAIJAJ&pg=6897.7259105&hl=en](https://news.google.com/newspapers?id=2245&date=19890814&id=FYQzAAAAIAJ&sjid=yzIHAIAAIJAJ&pg=6897.7259105&hl=en). August 14, 1989.


21 Their basic reason for opposition was that it was likely that the nuclear power used on the probe can eventually backfire and affect the Earth’s environment. Their fear was valid particularly due to what had happened to an earlier spacecraft called the Challenger. The Challenger though it was the second space shuttle to successfully reach space in April, 1983, also exploded less than two minutes after lift-off during its tenth launch in January, 1986. See Howell, Elizabeth. *Challenger: Shuttle Disaster That Changed NASA*. Retrieved from [http://www.space.com/18084-space-shuttle-challenger.html](http://www.space.com/18084-space-shuttle-challenger.html). October 16, 2012.

22 A computer worm is like a virus but more dangerous.


29 The Acteal Massacre took place in December, 1997 and saw the murder of 45 members of the Las Abeja, a small pro- EZLN pacifist group in Acteal, a small village in the Chiapas state of Mexico. The massacre was carried out by the Red Mask, a paramilitary group also based in Mexico. See Moksnes, Heidi. "Factionalism and Counterinsurgency in Chiapas: Contextualizing the Acteal Massacre." *Revista Europea de Estudios Latinoamericanos y del Caribe/European Review of Latin American and Caribbean Studies* (2004): 109-117.
31 Ibid.
32 Ibid. See page 75
36 Ibid.
37 Ibid.
40 Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
42 In simple terms, the users targeted other people and groups and ‘made fun’ of them.
44 Ibid.
45 Ibid.
47 Ibid.
49 Ibid.
51 Ibid.
CHAPTER THREE

The Implications of Hacktivism for International Relations

3.1 Introduction

This chapter firstly discusses the findings of this study with respect to how the hacktivism of WikiLeaks, Anonymous and Edward Snowden have affected international security. Secondly, attention is paid to presenting the findings regarding how the hacktivist activities of the actors falling within the scope of this study have directly caused states to embark on certain actions and take certain decisions towards other actors external to them within the international system.

3.2 The Implications of Hacktivism for International Security

This sub-section analyses the effect that hacktivism has had on international security. The discussion of the effects shall be limited to those resulting from the hacktivist activities of WikiLeaks, Anonymous and Edward Snowden. It must be said that it is the declassification of state secrets by these three hacktivists that have had the more significant relationship with national and international security. However, a few activities outside the declassification are also considered. The biggest leaks by WikiLeaks for instance were on the Afghan War, the Iraqi War and the diplomatic cables (popularly called ‘Cablegate’). All these leaks had a lot to do with security. Edward Snowden’s leaks were all about security. Anonymous which has a relatively more varied repertoire of leaks and attacks also has a significant portion of their activities bordering on security. The hacktivists have largely defended their actions by alluding to their interest in getting people to know about the activities of governments to ensure transparency. The reactions
of targeted states have largely concentrated on playing up the potential of such supposed transparency endangering national and international security. For example, in reacting to WikiLeaks’ activities, Joe Biden described Julian Assange as a “hi-tech terrorist”. Edward Snowden has been charged in absentia by the US for the; “theft of government property, unauthorised communication of national defence information and wilful communication of classified communications intelligence”.

3.2.1 Aiding terrorists and threatening International Security

Research has shown that terrorists have benefitted from the leaking of sensitive national security documents. The main argument of hacktivists is that by leaking into the public domain the classified information of governments, governments can be better held accountable. When people know what their governments are doing, they will stand in a better position to accept or reject the government and its policies. However, the public domain is membered by well-meaning citizens and terrorists. Thus whatever sensitive information is leaked can also be accessed by terrorists and tactically utilised. This is why Edward Snowden’s leaks of the surveillance methods of the NSA have been described in some conservative quarters as “a gift to terrorists”.

A study of the impact of the Snowden leaks conducted by a cyber-analytics firm, Recorded Future found that indeed terrorist organizations have derived some benefits form the Snowden-engineered revelations. According to the research, within a period of three to five months after the NSA’s surveillance tactics were exposed by Edward Snowden, at least three Islamic fundamentalist groups have designed improved versions of encryption tools. Encryption tools basically make it difficult for electronic
communications to be decoded and the communicators to be tracked. Specifically, the study revealed that the jihadist group GIMF in September 2013 released a new mobile encryption program called Tashfeer al-Jawwal for the Symbian and Android platforms. In November 2013, the Islamic State in Iraq and Syria released an encryption program called Asrar al-Ghurabaa after it had broken ties with Al-Qaeda. A major Al-Qaeda outfit, Al-Fajr Technical Committee (FTC) similarly released an encryption programme called Amn al-Mujahid in December, 2013. The graph below provides a visual representation of the trend of encryption development by jihadists post-Snowden.

Source: Recorded Future

A different report by Henry Jackson Society and authored by Robin Simcox also supports the conclusion that the Snowden revelations have aided the innovation by jihadists of encryption programmes that have made jihadists “harder to detect” as their “encrypted emails take longer to decipher”. Simcox also reports that post-Snowden; Islamic fundamentalist groups have resorted to using mobile phones and emails less and utilizing more human couriers. Simcox’s study concludes that “Snowden has helped terror suspects drop off the radar” and “…has caused severe damage to our [UK, US and their
counter-terrorism allies] ability to fight extremism”.\textsuperscript{8} It must however be said that not all studies concerning post-Snowden jihadists encryption come to the same conclusion. Flashpoint Global Partners for instance found that “the underlying public encryption methods employed by online jihadists do not appear to have significantly changed since the emergence of Edward Snowden”.\textsuperscript{9}

Officially, the US government has not publicly given the specific details of how these leaks can and/or have affected national/international security. This is regardless of the fact that a number of the members of the executive and legislature have consistently alluded in a very general manner to the security risks that the Snowden leaks have engendered. Notwithstanding, the US government released a document, which officially presents an impact assessment and impact projection of the Snowden leaks.\textsuperscript{10} The 39-page document however when it was released into the public domain, had a lot of paragraphs redacted resulting from a presidential order in the name of national security. The readable parts of the report present that “the scope of the compromised knowledge related to US intelligence capabilities is staggering” and that the Snowden leaks “will have a GRAVE impact on US national defense”.\textsuperscript{11}

One of the private documents belonging to Osama bin Laden that were confiscated by the US after capturing the former in 2011 and made public in 2015 details how Bin Laden sought to exploit WikiLeaks cables on Pakistan. Below is a quote from Bin Laden’s letter;

“Please dedicate some brothers to translate the documents on Afghanistan and Pakistan that were leaked from the Pentagon because these documents contain the strategy of the enemy in the area. The U.S. secretary of defense stated that the leak of these documents will negatively affect the
It will be difficult to prove how such an attention to the WikiLeaks cables aided the operations of Al-Qaeda but clearly its potential essence to the group cannot be overlooked especially in the light of Bin Laden’s words.

### 3.2.2 Fomenting mass protests and popular revolt

The leaks by hacktivists of government secrets provide citizens with an extraordinary insight into what their governments do behind the scenes. Such knowledge of government activities depending on their nature can inspire mass protests or popular revolts which can have varying implications for national and international security. A standout example of this is the Arab Spring. Basically, what is generally pointed to as the trigger of the Arab Spring is Mohammed Bouazizi’s self-immolation in Tunisia. The university graduate-turned-street hawker’s decision to burn himself in reaction to maltreatment by a police officer incensed Tunisians who had largely been suffering the effects of a harsh economy and entrenched corruption to protest against the government of President Ben Ali. Though this story is true, it downplays the role that hacktivism played in instigating the protests in Tunisia.

In 2010, WikiLeaks published thousands of classified cable correspondence authored mainly by US diplomats around the world. As part of these leaks were a number of cables authored by two US ambassadors to Tunisia from 2006 to 2008; Ambassador William Hudson and Ambassador Robert F. Godec. These cables generally contained the views of the two US diplomats on conditions in Tunisia particularly its governance and economy. The cables cast a damning verdict on Tunisia particularly President Ben Ali, his family
and business cronies and their unbridled corruption. The most famous of these cables came under titles such as:

“CORRUPTION IN TUNISIA: WHAT'S YOURS IS MINE”

“CORRUPTION IN TUNISIA PART I: AN ECONOMIC SUCCESS?”

“CORRUPTION IN TUNISIA PART II: THE ANATOMY OF EXPLOITATION”

“CORRUPTION IN TUNISIA PART III: POLITICAL IMPLICATIONS”

“CORRUPTION IN TUNISIA PART IV: THE FAMILY’S HOLDINGS”

The content of these cables detailed the pervasive corruption within the ranks of the ruling elite in Tunisia. These cables were published in late November, 2010 through December, 2010 on the WikiLeaks website as well as newspapers such as the Guardian in UK and two Arabic newspapers; al-Akhbar (Beirut) and al-Masry al-Youm (Egypt). Tunisians already knew that there was corruption in their country but the cables confirmed it and also showed the extent to which the canker had gotten. The cables kept indicating that despite the bad governance in the country, Tunisians were unlikely, mainly because of fear, to openly protest against their government.

However, as was later confirmed by the Foreign Minister of Tunisia at the time, Kamel Morjane, the leaked cables “did encourage people to speak in a more open and louder way”. This is because the Tunisians could sense from the cables that the US looked ready to withdraw its support from the Ben Ali regime. The perception that the US fully backed the regime had dissuaded Tunisians from openly opposing it. Notwithstanding, the content of the leaks incensed the average Tunisian and also encouraged him/her to challenge the government. Barely three weeks after the first publication of the Tunisia
cables, Bouazizi self-immolated and this heightened the anger that had built up in Tunisians due to the cables and the Arab Spring was born.

The Arab Spring spread through the Arab world and created a major international security challenge; overthrowing previously entrenched regimes in Tunisia, Egypt, Libya and Yemen. However, this came at the costs of a horrifying number of human lives, and massive infrastructural and economic destruction. It also incensed security stalemates in a number of countries like Libya, Yemen and Syria such that the world is still grappling with this legacy. The table below presents the death toll directly resulting from the Arab Spring as at July, 2011.

<table>
<thead>
<tr>
<th>Country</th>
<th>Status</th>
<th>Population, m *</th>
<th>Number killed, minimum</th>
<th>Deaths per m population</th>
<th>Period of unrest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syria</td>
<td>Ongoing revolution</td>
<td>20.4</td>
<td>1,300†</td>
<td>63.7</td>
<td>Mar 2011 - present</td>
</tr>
<tr>
<td>Egypt</td>
<td>Regime toppled</td>
<td>81.8</td>
<td>846</td>
<td>10.4</td>
<td>Jan - Feb 2011</td>
</tr>
<tr>
<td>Tunisia</td>
<td>Regime toppled</td>
<td>10.5</td>
<td>219‡</td>
<td>20.9</td>
<td>Dec 2010 - Jan 2011</td>
</tr>
<tr>
<td>Yemen</td>
<td>Ongoing revolution</td>
<td>24.1</td>
<td>2003†</td>
<td>8.3</td>
<td>Feb 2011 - present</td>
</tr>
<tr>
<td>Bahrain</td>
<td>Uprising crushed</td>
<td>1.3</td>
<td>29*</td>
<td>28.0</td>
<td>Feb - Jun 2011</td>
</tr>
</tbody>
</table>

Sources: Amnesty International; Egyptian Ministry of Health; OHR; UN Population Division press reports
*2010 estimates  †Excluding security force members  ‡Of which 72 reported linked to the unrest or in custody
§Excluding deaths resulting from clashes between security forces and other armed groups
**Of which 16 reported linked to the unrest or in custody

Sourced: The Economist.¹⁶

3.2.3 Promotion of citizen rights

Hacktivists have contributed to the direct protection of citizens in a number of countries across the world when their governments have chosen to blatantly crack the whip. States are tasked with the primary responsibility of ensuring the security of its people but there are many examples of cases in which the state itself endangers the security of its citizens.
Hacktivists have in such circumstances provided support to the oppressed citizenry. Thus hacktivism provides an opportunity for people outside a country to directly contribute to the safety of others in a transnational manner. This cross-border private individuals’ support mirrors in a way, the efforts of states and inter-governmental organizations to protect citizens of a state when its government is unwilling to. Anonymous has famously helped with the provision of such security in a significant way.

The first example of such support by Anonymous was in 2009 for Iranian protesters during the ‘Green Revolution’. When Mahmoud Ahmadinejad was announced as winner of the presidential elections in Iran in 2009, supporters of his opponent, Mir-Hossein Mousavi took to the streets in their numbers. The protesters believed that the elections had been rigged and that the leading opposition candidate should have been declared the winner. The Iranian government cracked down hard on the protesters and also blocked access to the internet especially social media websites like Facebook and Twitter. This attracted the attention of Anonymous which proceeded to form Anonymous Iran which was based on the website https://whyweprotest.net/. The website provided Iranian activists with tools and directions concerning how protesters can remain anonymous and avoid being detected by the government. The site also provided discussion forums which helped with the coordination of activities and in sustaining communication between the protesters and the outside world.

The second example was during the 2011 Arab Spring especially in Tunisia and Egypt. Like in Iran, the governments in Tunisia and Egypt responded to the mass protests by
blocking access to the internet. This tactic is often resorted to by oppressive governments for basically two reasons. The first is to weaken the effectiveness of the internet particularly its social media platforms in the mobilization of discontent and of protesters. Secondly, oppressive governments block access to the internet to ensure that the outside world does not easily get to know government excesses in their bid to control protesters and protests. Global knowledge of government violations of citizen rights essentially will cause the international community to place enormous amount of pressure on such oppressive governments. When governments blocked internet access in Tunisia and Egypt, Anonymous intervened and provided the protesters with means of circumventing these blockages like they had done in Iran.\(^{19}\) Anonymous protested against internet censorship in these countries by bombarding a number of government websites with DOS attacks and causing them to not function properly.\(^{20}\) Additionally, during the heat of the street protests in Egypt, Anonymous put together leaflets on how to treat tear gas effects and other basic medical conditions and faxed them to Egyptian protesters. This helped to promote the safety of the protesters and to sustain the protest.\(^{21}\)

3.2.4 Supporting global counter-terrorism efforts

Hacktivists have themselves been described as terrorists or at least aiding terrorism. Ironically, some hacktivists have in their own way helped to fight terrorism. In recent times, the terrorist group Islamic State in Iraq and Syria (ISIS) has been very active in the Middle East. The call by ISIS for global support in their bid to form a caliphate has been responded to with the springing up of splinter ISIS groups around the world and the swearing of allegiance to ISIS by Islamic fundamentalist groups which already existed. Also, a lot of foreign fighters have moved from their countries to join ISIS. One very
influential factor in the growth of ISIS has been the group’s use of the internet, particularly social media. Research shows that the period from September through December 2014 saw the operation of over 46,000 pro-ISIS accounts on Twitter.\(^2^2\) This number is significant though not all of them were active at the same time. These pro-ISIS accounts have been dedicated to spreading the message of ISIS, popularizing the activities of the group, radicalizing internet users and recruiting foreigners to join ISIS in its fight. Such pro-ISIS accounts also hack into accounts belonging to ‘enemy’ organizations and post threatening messages.

Anonymous led by a sub-group within it called GhostSec (Ghost Security in full) has responded by waging a cyber-war on ISIS in a campaign called #OpISIS. With this cyber-war, Anonymous has targeted pro-ISIS accounts and closed them down one after the other. In April 2015, Anonymous released a list of 14,000 pro-ISIS twitter accounts and 70 pro-ISIS websites as well as the names of companies in the US and UK hosting these websites.\(^2^3\) According to Anonymous they are targeting accounts “frequently used by the Islamic State through Twitter and other social media platforms for transmission of propaganda, religion, recruitment, communications and intelligence gathering purposes”.\(^2^4\)

Some state security agencies have indicated that the extermination of pro-ISIS social media accounts and websites by Anonymous hinder their efforts to gather intelligence. Anonymous has responded by indicating that these accounts are basically used for propaganda purposes and for spreading fear and not necessarily for disseminating
military or strategic information. Notwithstanding this debate, the Anonymous campaign against ISIS on the internet is likely to have positive repercussions for the global fight against the fundamentalist group. This is because, closing down such pro-ISIS accounts hinders the efforts by ISIS members and supporters to use the internet particularly to radicalize internet users, recruit foreign fighters and spread propaganda and fear.

According to the United Nations, about 25,000 foreign fighters from over a 100 countries have joined terrorist groups in the period beginning from the middle of 2014 to March, 2015. The UN report indicates that about 20,000 of the number joined particularly ISIS in Iraq and Syria. In the light of this, the American government has been impressed upon to collaborate with and support Anonymous in its cyber war on ISIS especially as members of Anonymous seem sufficiently adept given the terrain.

3.2.5 International Security Reform

Hacktivism has inspired in a significant manner, an active discourse on security reform especially with regards to mass surveillance. The three hacktivists this work focuses on have particularly played stand-out roles in instigating this discourse on security reform. Generally, the major issues in this discourse on reform have revolved around questions like; can the state spy on its own citizens and to what extent; can the state spy on friendly countries and their leaders; to what extent can the details of mass surveillance be known to the public; and how should a hacktivist who makes public classified state information be dealt with. There have been national and regional efforts to reform surveillance guided by the foregoing questions. These targeted reforms seek to shape the nature of international security particularly on the front of mass surveillance, inter-state spying and
the relations between the state and a hacktivist. Some of such reform efforts are highlighted after here. It must be said that the reform process is still rolling in many instances.

3.2.5.1 The European Court of Justice (ECJ)

In April 2014, the ECJ in a landmark case ruled that the European Union’s data collection laws are illegal. In 2006, as a post 9/11 and post Madrid/London bombings counterterrorism measure, the European Union passed the Data Retention Directive law. This law mandated telecoms to store the communications of their clients with the view that such information can effectively help in the fight against terrorism. However, with the Snowden leaks revealing massive intrusion of citizens’ communications by governments, the ECJ ruled that the Data Retention Directive law is illegal as it “entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary”. This ruling significantly seeks to change the dynamics of data collection by European intelligence agencies.

3.2.5.2 The European Union’s Committee on Civil Liberties, Justice and Home Affairs

In 2013, after the Snowden leaks, the afore-mentioned committee held an enquiry and released a report on the US NSA surveillance programme as well as surveillance bodies in various EU member states and their impact on European Union (EU) citizens’ fundamental rights and as well as on transatlantic cooperation in Justice and Home Affairs. The committee made crucial recommendations for reform. These recommendations included calls;
“…on Member States to take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on EU Member States to make use of all available international measures to defend EU citizens’ fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of the International Covenant on Civil and Political Rights (ICCPR)…”

“…on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens and to sign the Additional Protocol allowing for complaints by individuals under the ICCPR…”

3.2.5.3 UK has passed a Data Retention and Investigatory Powers Act (DRIPA)

After the ECJ ruled to affirm the illegality of a blanket approach to surveillance, the UK government quickly pushed through the DRIPA in the UK Parliament. It was placed before parliament and passed all in the space of one day. The DRIPA basically insulates British intelligence agencies from the effects of the ECJ ruling against the Data Retention Directive law. As such, UK telecoms and Internet Service Providers are bound to retain the details of people’s electronic communication for 12 months so that they can be used by UK security agencies in their investigations as and when necessary. Here you find the Snowden pressure rather leading to a legal entrenchment of intrusive surveillance in the name of national security. However, in July 2015, a UK high court ruled that the DRIPA was unlawful as it is “inconsistent with European Union law” and as such ordered the UK Parliament to rewrite the law to tighten the oversight on security agencies that operationalize the law in their work.

3.2.5.4 The UK Parliament’s Intelligence and Security Committee (ISC)

The ISC enquired into allegations that UK intelligence agencies in their mass surveillance were violating the law. The ISC’s report concluded that intelligence agencies did not break any law. However, the ISC indicated that as the legal framework governing
surveillance in the UK, has “developed piecemeal, and is unnecessarily complicated”, there were “serious concerns about the resulting lack of transparency, which is not in the public interest”. As such, the ISC recommended that “the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so”. Here, one finds the Snowden leaks leading to processes to streamline within the remit of the law, the surveillance work of national security setups in the UK.

3.2.5.5 America’s Signals Intelligence Reform 2015 Report

There have also been efforts in America to ensure reform with regards to surveillance post the Snowden leaks. The Signals Intelligence Reform 2015 Report is only one of the documents that discuss such reforms. The reforms include the following; the establishment of an oversight board to supervise the spying by American intelligence agencies on foreign leaders; where incidental information on Americans are found when monitoring foreign targets, the information on the American citizen should be purged if it contains no useful intelligence; purging useless records on foreigners after a period of five years; and making public National Security letters meant to gag companies after three years.

Beyond these measures, the Snowden leaks led to what The Guardian described as the “first surveillance reform in a decade” in the United States. This was said in reference to the passing of the USA Freedom Act in June, 2015 which was undoubtedly inspired by the Snowden leaks more than anything else. The Act basically seeks to;

“end the mass collection of Americans’ phone records by the NSA, restore some expired powers to security agencies, place record storage in private companies’ hands, create a public-interest
This is further evidence that indeed the revelations by hacktivists have pushed states to embark on reform measures particularly in relation to mass surveillance.

3.3 The Implications of Hacktivism for Inter-State Relations

Foreign policy has been defined variously by several scholars. Frankel for instance, defines foreign policy as “decisions and actions which involve to some appreciable extent relations between one state and others”. Marshall also defines it as “the course of action undertaken by authority of a state and intended to affect situations beyond the span of its jurisdiction”. Going by these definitions, it is clear that foreign policy is made by the state and targeted at other states and indeed any other group that does not fall under the jurisdiction of the said state. Foreign policy generally refers to the actions and decisions of a state aimed at achieving its national interests and targeted at parties or actors that are external to it. Thus foreign policy guides or streamlines foreign relations in the promotion of the national interest. The external actors targeted by foreign policy include states and foreign non-state actors such as multinational corporations as well as inter-governmental organizations and international non-governmental organizations.

Thus for the purposes of this section, the focus principally is on how the hacktivism of WikiLeaks, Anonymous and Edward Snowden have directly caused states to take decisions and embark on actions in the international realm in relation to other states. The attention here is on how hacktivism has gotten states to maintain, improve or sever some foreign relations. This sub-section will proceed to show how hacktivism has influenced
states in their conduct of foreign relations. The approach will be to discuss the findings under country themes; how some countries had their foreign relations affected. Countries have been selected and discussed mainly because not all states can be discussed given the space for this work. Secondly, the countries chosen have been some of the most prominent in terms of issues to do with the hacktivism of WikiLeaks, Anonymous and Edward Snowden.

3.3.1 USA

For all it is worth, the United States has been the most notable country in the hacktivism discourse. The hacktivism particularly of WikiLeaks and Edward Snowden had more to do with the United States than any other country. Indeed, the leaking of the Afghan War Logs, the Iraqi War Logs and the diplomatic cables by WikiLeaks had the chief objective of exposing the United States in order to cause it to amend aspects of its foreign policies. The revelations by Edward Snowden had the same objective. On the flipside, the exposures also held the potential of getting other states to alter their relations with the United States or push the United States to make such alterations. Some of the more open foreign relations fallouts for the United States are highlighted hereafter.

First of all, the WikiLeaks revelations of hitherto classified diplomatic cables authored by US diplomats around the world caused Hillary Clinton, the then Secretary of State to embark on what she herself tagged as the “apology tour” of the Middle East. The cables had revealed several conversations detailing what leaders of Middle Eastern countries had said in confidence to US diplomats. Naturally, the cable leaks symbolized a major
breach of confidence and the US rightfully feared that it was going to cost them dear in their relations with Middle Eastern countries. Thus the US quickly reacted by embarking on this apology tour to save their alliances in the Middle East.

Secondly, the leaks led to a shakeup in America’s diplomatic circles. Some US diplomats ended up being reassigned for what they had written about the government or leader of the country that they were serving in. Gene Cretz who at the time of the leaks was serving as America’s ambassador to Libya was reassigned in January, 2011. Cretz had written several unflattering cables about Gadhafi and his family. According to an anonymous US state representative; US-Libya relations was already “a complicated relationship, and WikiLeaks just added to that complication”.\(^{42}\) Cretz was appointed to serve in Libya in 2008; the first such appointment since 1972. Similarly, Sylvia Reed Curran who served as the charge d'affaires in Ashgabat, Turkmenistan was reassigned.\(^{43}\) Curran had also been exposed by the leaks to have written a very harsh report about the President of Turkmenistan, Gurbanguly Berdimuhamedow.\(^{44}\)

In March 2013, Carlos Pasqual resigned as America’s ambassador to Mexico. Pasqual had been quoted in the leaks to have said that Mexico’s President, Felipe Calderon and his government in general had been lukewarm and even less concerned regarding the fight against drug trafficking in Mexico. Pasqual formally resigned as ambassador due to the angst that his leaked cable had caused within the Mexican government.\(^{45}\) His resignation was “to avert issues raised by President Calderon that could distract from the important business of advancing our [US and Mexico’s] bilateral interests”.\(^{46}\) It has been
reported that President Calderon had pushed the US to reassign Pasqual.\textsuperscript{47} In that light, Pasqual’s resignation was America’s diplomatic way of taking Pasqual out of Mexico and posting a new person to Mexico to save the bilateral relations of the two North American neighbours.

Also, the Iraq War logs has been said to have contributed to the pull-out of US soldiers from Iraq in 2011. The US and Iraq had earlier agreed that the former would pull its troops out of Iraq in 2011; however US had embarked on talks with Iraq to keep their troops in Iraq beyond 2011. The US government as a condition for extending its stay pressed for Iraq to provide their soldiers with immunity. The Iraqis rejected the idea of such immunity particularly because of the revelations of WikiLeaks detailing several abuses including extrajudicial killings and indiscriminate civilian killings by the US army and its partners. Particularly, according to Cable News Network (CNN), “the negotiations were strained following WikiLeaks' release of a diplomatic cable that alleged Iraqi civilians, including children, were killed in a 2006 raid by American troops rather than in an airstrike as the U.S. military initially reported”\textsuperscript{48}.

In 2014, three years after CNN had reported similarly, President Obama sensationally asserted that withdrawing US troops from Iraq was not his decision. His subsequent explanation thinly fell short of confirming the impact of the WikiLeaks revelations on the pull-out. According to President Obama;

\begin{quote}
“\textquote{In order for us [the US] to maintain troops in Iraq, we needed the invitation of the Iraqi government and we needed assurances that our personnel would be immune from prosecution if, for example, they were protecting themselves and ended up getting in a fire-fight with Iraqis, that they wouldn’t be hauled before an Iraqi judicial system. And the Iraqi government, based on its}
\end{quote}
political considerations, in part because Iraqis were tired of a U.S. occupation, declined to provide us those assurances”\(^{49}\).

The Iraqi logs had revealed the huge number of civilians that had been killed by US soldiers and a number of other human right infringements. Thus it is no surprise that there was an absence of popular support for the US troops’ continued stay in Iraq. This meant that the Iraqi government did not have the political capital to allow the American troops to stay and on top of that, grant them immunities. This dwindled political capital in turn affected America’s policy in terms of staying in Iraq.

Also the Snowden revelations in 2013 affected the conduct of US’ external relations. This was for instance clearly shown when President Obama cancelled a scheduled bilateral meeting with President Putin in Moscow in August, 2013 ahead of a G 20 summit in St. Petersburg the following month. One of the main reasons (if not the main reason) why the United States called off that meeting was because Russia had at the time, granted Edward Snowden temporary asylum. According to official US government communication;

"Russia's disappointing decision to grant Edward Snowden temporary asylum was also a factor that we considered in assessing the current state of our bilateral relationship. Our co-operation on these issues remains a priority for the United States"\(^{50}\)

Edward Snowden had been charged with treason by the US and President Obama described Russia’s decision to harbour Snowden notwithstanding as symbolizing Russia’s habit of slipping back every now and then into “cold war thinking and a cold war mentality”\(^{51}\).

3.3.2 Brazil

Edward Snowden’s revelation that the United States had been over-reaching in its international counter-terrorism surveillance incensed many countries and world leaders
around the world. The anti-America public outcry in Brazil for instance, was very intense because in the case of Brazil, its natural and legal persons had been targeted by the NSA. The last straw was the revelation that President Rousseff had herself had her email and telephone conversations tapped by the United States. The distaste of the whole situation caused Brazil to react strongly in the international realm. Brazil put in place an Investigative Parliamentary Commission for inquiry into the Snowden revelations.

In September 2013, President Rousseff cancelled what would have been the first visit by a sitting Brazilian President to the United States since 1995. This action was explained in a public statement by the Brazilian government as resulting from the fact that;

“illegal interception of communications data belonging to citizens, companies and members of the Brazilian government are a grave matter, an assault on national sovereignty and individual rights, and are incompatible with relations between friendly nations”.52

This action was indeed a major declaration of intent in Brazil’s relations with the United States. After calling off the meeting with President Obama, President Rousseff proceeded to intensify her pressure on the United States by delivering a fiery speech before the 68th United Nations (UN) General Assembly which was clearly a frontal attack on the United States. Concerning the NSA’s intrusive cross-border surveillance Rousseff asserted that;

“Tampering in such a manner in the affairs of other countries is a breach of International Law and is an affront to the principles that must guide the relations among them, especially among friendly nations. A sovereign nation can never establish itself to the detriment of another sovereign nation. The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country…”53

“…[Brazil] will redouble its efforts to adopt legislation, technologies and mechanisms to protect us from the illegal interception of communications and data. My Government will do everything within its reach to defend the human rights of all Brazilians and to protect the fruits borne from the ingenuity of our workers and our companies”54.

61
President Roussseff used the opportunity to call for multilateral efforts aimed at curbing such over-reaching intrusions, regulating sovereignty in cyberspace and entrenching digital rights of individuals across the world. The position of this speech and actions Brazil subsequently took showed the extent to which Brazil was using the Snowden revelations as an opportunity to become a world leader in the issue of entrenching the digital rights of individuals. This was evident in Brazil’s lead role (alongside Germany) in drafting a UN resolution accepted by consensus in December, 2013 entitled ‘Right to Privacy in the Digital Age’.\(^5\)\(^5\) The resolution which was also adopted in December 2014 but this time with 35 more co-sponsoring member-states seeks to entrench the digital communication rights of individuals around the world.\(^5\)\(^6\)

At home, Brazil also passed the ‘Marco Civil da Internet’ legislation in March, 2014. The law which already existed as a bill from 2009 was quickly made law after the exposé on the NSA surveillance. The Marco Civil generally provides a legal basis for the protection of the digital communication rights of Brazilians and Brazilian institutions. It has been described as the Magna Carta or the Bill of Rights for the Internet.\(^5\)\(^7\) By the law, the private digital communication of Brazilians should not be intercepted by any other party as that would be tantamount to a violation of rights. Though this is basically a domestic policy, there is a foreign policy angle to it. By the law, all digital communication by Brazilians stored on non-Brazilian servers which are located inside or outside Brazil cannot be intercepted.\(^5\)\(^8\) In this light, internet companies such as Facebook, Twitter and Google among others cannot intercept online interactions by Brazilians or hand them over to a third party (like their home governments). Initially, the Marco Civil as a bill
sought to even ask internet companies to build local servers in Brazil purposely to store the digital communication of Brazilians.\textsuperscript{59}

\textbf{3.3.3 Ecuador}

Ecuador has also seen hacktivism shaping its foreign relations particularly with the United States. For starters, Ecuador was the only country that explicitly expelled a foreign ambassador from their country following the ‘Cablegate’ revelations. In April 2011, US ambassador Heather Hodges was expelled by Ecuador. Hodges had claimed in the leaked cables that there was deep-seated corruption within the Ecuadorean police force and cited President Correa as being aware of this and not acting on it.\textsuperscript{60} Ecuador tagged the allegations as "absolutely irresponsible and false". After expelling Hodges, Ecuador explained that the ambassador was expelled as she could not give any satisfactory explanations for her claims.\textsuperscript{61}

In 2010, two women in Sweden accused Julian Assange of sexual offences. At the time, Assange was based in the UK and as such, the Swedish government asked the UK to extradite Assange to Sweden and the former was willing to extradite. However, the sex offence case, Sweden’s pursuit of Assange and the UK’s willingness to extradite were interpreted by some as witch-hunting against Assange for the many WikiLeaks exposés. To conspiracy theorists, it was likely that a UK extradition of Assange to Sweden would be followed by an extradition of Assange by Sweden to face espionage charges in the United States with the possibility of a death penalty being meted out to Assange. In June 2012, Assange sought asylum in the Ecuadorean embassy in the UK and in August that
year, Ecuador officially granted Assange the asylum despite huge pressure from the UK. At this point, the UK made it clear that it was willing to invoke a domestic law, the Diplomatic and Consular Premises Act 1987 to scrap the immunity of Ecuador’s embassy premises in order to arrest Assange. As pointed out by a former Ecuador ambassador to the UK at the time, “What Ecuador is doing is a very delicate thing… Ecuador is risking its economic interests for this adventure of defending Mr. Assange.”

After Edward Snowden escaped from the United States, he was charged with treason, his passport was revoked and was seeking asylum from a number of countries around the world. As mentioned earlier, Russia eventually provided him the asylum. However, some countries particularly Venezuela, Bolivia and Nicaragua openly indicated their openness to the idea of providing Snowden with asylum. Ecuador at a point indicated that they were contemplating harbouring Snowden just as they have done for Assange. This position was met with threats from the United States. Senator Robert Menendez, the leader of the U.S. Senate Foreign Relations Committee, for instance threatened that the US government would re-evaluate the trade benefits being given to Ecuador. U.S. Trade Representative Michael Froman posited similarly. The Andean Trade Promotion and Drug Eradication Act enacted in 2002 gives duty-free access to a lot of goods from Bolivia, Colombia, Ecuador and Peru to the United States. In exchange, these countries are expected to help the United States in a crackdown on the production and proliferation of narcotics. However, incensed by the attempts by the US to use the Act as a weapon of political pressure; Ecuador in June, 2013 opted out of the programme. Ecuadorean President, Rafael Correa to this end, declared;
"All of a sudden, trade tariffs became an instrument of blackmail: behave or leave the free trade movement. In the face of threats, insolence and arrogance of certain U.S. sectors, which have pressured to remove the preferential tariffs because of the Snowden case, Ecuador tells the world: We unilaterally and irrevocably denounce the preferential tariffs. Our dignity has no price".

3.3.4 Germany

Germany is one of the countries that conducted a parliamentary enquiry into the Snowden revelations. As was briefly mentioned earlier in this section, Germany co-sponsored with Brazil, the first UN resolution aimed at protecting the privacy of the digital communication of individuals. One of the biggest revelations by Edward Snowden was that the NSA was spying on Germany, a country that is a major ally of the United States. The more shocking part was that, German Chancellor had for years being spied on by the NSA; her emails and phone calls had been tapped. Thus it was not surprising that Germany co-sponsored a UN resolution basically targeted at the United States. On the heels of this, Germany also has been pushing for an additional or optional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (which enshrines the right to privacy) to include specifically and explicitly, the protection of the digital communication of people and organizations.

In August 2013, revelations by Edward Snowden caused Germany to cancel a spying pact that it had with the United States and the UK during the Cold War in 1968/1969. The pact gave the right to UK and the US which had military forces stationed in Germany the right to request for the permission to embark on surveillance within Germany to protect their troops. In the words of the then German Foreign Minister, Guido Westerwelle, the cancellation was “a necessary and proper consequence of the recent debate about...
protecting personal privacy”. In July 2014, Germany also took the stern decision of expelling the head of US intelligence services in Germany.

Last but not least, ever since the Snowden revelations, Germany has publicly declared its intention and efforts towards brokering a ‘no-spy agreement’ with the United States. Presently, the US has such an agreement with the four other member-states of the ‘Five Eye’; Australia, UK, Canada and New Zealand. As such, the US is not supposed to spy on these four countries and vice versa. Germany posits that it is an equally strong ally of the US and as such must be given the same treatment. Though Germany has been talking up its efforts towards gaining such an agreement, the US has not as it stands, agreed to it.

3.3.5 Austria

In July 2013, the plane of Evo Morales, President of Bolivia was forced to land and was searched by Austria in Vienna. This was a major decision and largely unconventional in diplomatic circles. It took 12 hours before Morales was allowed to continue his journey. Morales was returning from a visit to Russia and as mentioned earlier in this sub-section, Bolivia alongside Nicaragua and Venezuela had openly declared that they would look on favourably to any request by Snowden to seek asylum in their countries. At the time, Snowden was in Moscow. As such, there was the assumption on the part of the United States and its allies that Morales’ plane could likely have on board, Edward Snowden.

Thus according to Bolivia; France, Italy and Portugal all refused to allow Morales’ plane to land in their countries to refuel. It is likely that these countries were been pressurized
by the US to search the plane if it landed in their territories and realizing the innate lack of diplomatic courtesy with such an act as well as fearing the consequent backlash, they rather preferred that Morales’ plane would not land in their territories at all. In this light, the decision by Austria to force Morales’ plane to land and search it all in the name of finding Edward Snowden was a risky foreign policy decision on their part which sort to place more regard on Austria’s bilateral relations with the United States while virtually disregarding and endangering Austria’s relations with Bolivia.

To conclude, this chapter has presented and discussed a number of implications that hacktivism has had for international security and inter-state relations. The next chapter presents a summary of the research findings, conclusions and recommendations.
Endnotes

3 This is according to MI5 Director, General Andrew Parker. See “British Spy Chief warns Snowden data is a ‘gift’ for terrorists”. Reuters. http://www.reuters.com/article/2013/10/08/us-usa-security-britain-idUSBRE9711A20131008, Oct 8, 2013.
5 Ibid.
6 Ibid.
8 Ibid.
9 Ibid.
11 Ibid.
13 Excerpts from one of such cables: “In summer 2007, Leila Ben Ali received a desirable tract of land in Carthage for free from the GOT in order to build the for-profit Carthage International School (Ref F). In addition to the land, the school received a 1.8 million dinar (US $1.5 million) gift from the GOT, and within a matter of weeks the GOT had built new roads and stoplights to facilitate school access. It has been reported that Ms. Ben Ali has sold the Carthage International School to Belgian investors, but the Belgian Embassy has as yet been unable to confirm or discount the rumour. XXXXXXXXXXXX asserted that the school was indeed sold for a huge, but undisclosed sum. He noted any such sale would be pure profit since Ms. Ben Ali’s received land, infrastructure, and a hefty bonus at no cost”. See in Godec, Robert. “Corruption in Tunisia: What’s yours is mine”. WikiLeaks. 
14 The Secret Life of a Superpower, Episode 1 - WikiLeaks - BBC Two Documentary. 
http://www.youtube.com/watch?v=BeG-13y2y3g, 2013.
15 Ibid.
18 “Anonymous Joints Fight Against Tyranny In Iran”. Business Fundit. 
20 Ibid.
21 Ibid.
26 Ibid.
31 Ibid.
35 Ibid.
38 Ibid.
44 Curran described Gurbanguly as “vain, suspicious, guarded, strict, very conservative”, a “micromanager” and “a practised liar” and that “Berdyumukhamedov does not like people who are smarter than he is. Since he’s not a very bright guy, our source offered, he is suspicious of a lot of people.” See Ibid.
46 Ibid.
47 Ibid.

51 Ibid.


54 Ibid.


59 Ibid.


61 Ibid.


66 Ibid.

67 Article 17 of ICCPR states that: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks. See UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: http://www.refworld.org/docid/3ae6b3aa0.html


69 Ibid.

70 Ibid.


CHAPTER FOUR

Summary of Findings, Conclusions and Recommendations

4.1 Summary of Findings

This chapter presents a summary of the findings of the study and the conclusions drawn based on the findings. The chapter also presents some recommendations particularly for researchers who may in the future be interested in carrying out studies related to hacktivism and international relations. This work set out to basically provide an overview of hacktivism and also to answer three major research questions; the implications of hacktivism for: international security and inter-relations. The theory that guided the study was pluralism which basically challenges the realist assertion that states are the only significant actors in the international system. Pluralism posits that non-state actors can also be significant actors in the international system. The theory was chosen because the hypothesis of this study indicates that hacktivists (who are non-state actors) have had an influence on international security and inter-state relations.

The hacktivists that were studied were WikiLeaks, Anonymous and Edward Snowden. The three actors were chosen because of the amount of coverage they have enjoyed in the media. Indeed, the mention of hacktivism everywhere is very likely to first bring these three actors to mind. As such, it stood to reason that a study of the implications that hacktivism has had for international relations would not overlook these three actors. The study was based on qualitative methodology. More specifically, the approach of document analysis was utilized. The study resorted to secondary data carried in journal
articles, books, reports, press releases/statements, video documentaries and news articles relevant to the topic for its analysis and the subsequent deduction of findings. The findings of the study are presented hereafter.

4.1.1 Implications of Hacktivism for International Security

Here, the study was primarily interested in finding out how in practical terms, hacktivism has impacted international security. The summary of the findings are presented hereafter.

Aiding terrorists and threatening International Security: Revealing the classified security plans and approaches of states can lead to terrorists and other criminals taking advantage and endangering international security. Research has for example pointed to the fact that revelations of US surveillance methods has coincided with an increase in the development of better encryption software by a number of jihadi groups.

Fomenting Mass Protests and Popular Revolt: The leaks by hacktivists of government secrets provide citizens with an extraordinary insight into what their governments do behind the scenes. Such knowledge of government activities depending on their nature can incite or incense mass protests or popular revolts which can have varying implications for national and international security. A standout example of this is the Arab Spring as it happened in Tunisia. Beside the self-immolation of Muhammed Bouazizi, the Arab Spring protest in Tunisia (in terms of catalysing factors) has also been linked to revelations by WikiLeaks detailing the corruption of the Ben Ali government and crucially, exposing America’s willingness to withdraw their support for the Ben Ali regime.
**Promotion of Citizen Rights:** Hacktivists have also showed that they can help promote human rights internationally. There are two sides to this. Firstly, the key objective of hacktivists has always been to promote the right of citizens to information by exposing what governments and indeed other actors do behind the scenes that can particularly threaten the wellbeing of citizens. Beyond that, when oppressive governments have tried to clamp down on popular dissent, hacktivists have in some instances engineered mechanisms to protect the rights of these citizens. For example, when the Iranian government shut down the internet in 2009 during the Green Revolution, Anonymous provided the Iranian protesters with means to circumvent the internet blockade in order to mobilize and keep the protest going as well as keep revealing to the world the high-handedness of the Iranian government’s clampdown. Similarly, Anonymous kept the internet open to protesters in Tunisia and Egypt during the Arab Spring when the governments in the two countries blocked access to the internet. Beyond internet access, Anonymous provided support to protesters in Egypt during the Arab Spring by supplying the protesters with pamphlets detailing practical ways of protecting one’s self from the harm of tear gas as well as some helpful first aid practices.

**Supporting Global Counter-Terrorism efforts:** Hacktivists have in their own way helped to fight terrorism. Positively, for example, Anonymous led by its sub-group called GhostSec (Ghost Security in full) has waged a cyber-war on ISIS in a campaign called #OpISIS. With this cyber-war, Anonymous has targeted pro-ISIS accounts and has been closing them down one after the other. Such an effort has heavily clamped down on pro-
ISIS accounts that have been dedicated to spreading the message of ISIS, popularizing the activities of the group, radicalizing internet users and recruiting foreigners to join ISIS in its fight. The effectiveness of this effort has led to calls for the US government for instance to work with Anonymous in waging a cyber ‘war’ on pro-jihadi internet websites and social media accounts.

**International Security Reform:** Hacktivism has inspired in a significant manner, an active discourse on security reform especially with regards to mass surveillance. The three hacktivists this study focused on have particularly played stand-out roles in instigating such a discourse on security reform. The reforms will go to shape the nature of international security particularly on the front of mass surveillance, inter-state spying and the relations between the state and the hacktivist. For example, following Snowden’s revelation of massive intrusion of citizens’ communication by governments, the European Court of Justice proscribed the EU’s Data Retention Directive law. This ruling sought to protect the privacy of the communication of individuals within EU member-states.

**4.1.2 Implications of Hacktivism for Inter-State Relations**

Here, the focus principally was on how the hacktivist activities of WikiLeaks, Anonymous and Edward Snowden have directly caused states to take decisions and embark on actions to pursue/safeguard their national interests within the international system. Instances of such foreign relations moves were seen in the US, Brazil, Ecuador, Germany and Austria. For example, the leaks by the studied hacktivists led to a shakeup
in America’s diplomatic circles. In less veiled words, the revelations from the ‘cablegate’
caused some American diplomats to be reassigned for what they had written about the
country or leader of the country that they were serving in. Gene Cretz who was
America’s ambassador to Libya was reassigned. Sylvia Reed Curran who served as the
charge d'affaires in Ashgabat, Turkmenistan was reassigned. Mexico pushed for the
resignation of the US ambassador, Carlos Pasqual. In April 2011, Ecuador had the US
ambassador Heather Hodges expelled. The Iraq Logs leaked by WikiLeaks also
contributed to the US withdrawing its troops from Iraq at the time and in the manner it
was done. President Obama cancelled a meeting with Vladimir Putin because Russia had
agreed to provide Snowden with asylum. In Brazil, the Snowden leaks led to President
Dilmar Rousseff also cancelling a crucial meeting with President Obama in Washington
as a strong show of protest against the US’s surveillance of Brazilian leaders and
industries.

4.2 Conclusions

Based on the findings, the following conclusions are made.

- It can be concluded from this study that as posited by the theory of pluralism,
  aside states, non-state actors play a significant role in the international system.
  The power of hacktivists is immense as they can sit in one country and utilize
  communication technology to affect international politics. This fits into the
  conception of pluralism by the likes of Robert Keohane, Joseph Nye and Arnold
  Wolfers. For example, hacktivists fall into the class of non-state actors that
  Wolfers asserts are “able on occasion to affect the course of international events”
and as such, become “actors in the international arena and competitors of the nation-state”.\textsuperscript{1} Being competitors of the nation-state suggests that states are not unitary actors. There are other sub-state actors like hacktivists who hold views and pursue actions that oppose those of the state. This position is similarly held by pluralists like Keohane and Nye.\textsuperscript{2} Again, another assumption of pluralism that is confirmed by the findings of this study is that military issues are not the only significant issues for states in the international system. As proven by this study, issues like governance, trade and human rights are also significant for states in the international system.

- In terms of inter-state relations, the declassification or leaks by hacktivists seem to have more impact than the use of other hacktivist tools like website defacements and DOS attacks among others.

- Regarding international security, there is a very high likelihood that there are many ramifications that hacktivism has had. States and other organizations have likely changed a number of security measures in response but for obvious reasons cannot be declared in the public domain.

- Finally, the hypothesis for this study has been proven by the work as partly positive and partly negative. Hacktivism has had positive implications for international security but negative implications for inter-state relations. First of all, regarding international security, as has been shown in this study and contrary to commonly held assumptions, hacktivism has done more to improve international security than threaten it. The push for the entrenchment of the rights to digital privacy, the cyber-wars against jihadi groups as well as reforms towards
bringing mass surveillance under control and bringing under control war-time military excesses among others, serve as evidence to this conclusion. However, regarding inter-state relations, it can be seen that the revelations of state secrets by hacktivists has incited a lot of tensions in the short-term. Examples are the Iraq War Diaries, Afghanistan War Logs and the ‘Cablegate’, among others. Some of the declassified documents have exposed the abuses of the sovereignty and territorial integrity of states by other states. The ‘victim’ states have naturally reacted strongly; summoning foreign diplomats to provide answers; at times pushing for the recall (or even expelling) foreign officers; cancelling scheduled diplomatic engagements; abrogating already established defence agreements and trade pacts among others. Also, the attempts by some states to punish hacktivists and the attempts by other states to harbour and protect the same hacktivists, have also further strained relations between the states involved. This contradicts the position held by some authors in the literature that hacktivism has had or can have relatively negligible impact on diplomacy. The concern of these authors including Robert Saunders, Mark Page and Spence has been on whether states will continue to interact with each other in the same way after revelations by hacktivists and have concluded in the affirmative.\(^3\) As this research has shown, states have not ended diplomatic ties due to such revelations but clearly, inter-state relations in a number of instances have been strained at least in the short to medium term. This confirms the position held by Nicholas Cull that the hacktivism of WikiLeaks has been a “game-changer”.\(^4\)
4.3 Recommendations

This sub-section proceeds to make recommendations regarding the utility of hacktivism and for future research in the area of hacktivism and international relations.

- Thus far, hacktivism has incited a number of moves for reform particularly in terms of security in many states. To this end, it is about time that the conception of hacktivists as criminals particularly on the part of states is given a second thought.

- The efforts by hacktivists like Anonymous to wage a cyber-war against terrorist organizations as has been shown in this work are positive. The point has been established that the skill of such hacktivists in that light may be more than that of state security agencies or at least close. To this end, states can utilize the capacity and resource of hacktivists and collaborate with them to track and sustain the cyber-war on terrorists and other criminal organizations.

- The revelations by hacktivists of state secrets provide an opportunity for states to reassess their relations with other states and pursue or even demand certain changes. Such a pursuit seeks to improve bilateral relations and make it more mutually beneficial. Similarly, they provide an avenue and even some much needed evidence for non-state actors to utilize and demand changes particularly with respect to issues of human rights from governments.

- The literature on hacktivism reveals a disproportionate emphasis on its connections to the US. Though this is understandable because many of the major hacktivist agenda have targeted the US, it is important for more attention to be
paid to interpreting hacktivism as it relates to other countries, particularly in the developing world.

- Hacktivists like WikiLeaks, Edward Snowden and Anonymous present a relatively new kind of non-state actor as they can sit in a room and affect policy-making worldwide. It will be important for more emphasis to be placed on understanding and building theories specifically explaining the role and actions of such actors in the international system.

- The advent of WikiLeaks has particularly incited the formation of other similar organizations dedicated to pushing for government transparency and accountability through similar means like GhostShell in South Africa. In the light of this, it will be important to investigate the operations and the success or otherwise of such new hacktivists.

Efforts towards putting into practice the first three recommendations listed above will go a long way to engender a positive collaboration between hacktivists and other actors in the international system including states. Importantly also, the research-related recommendations that follow, if pursued can promote the utility of the academic literature on hacktivism. This chapter has presented a summary of the findings and conclusions for the study as well as a number of recommendations. In all, this study has assessed the implications that the hacktivism of WikiLeaks, Anonymous and Edward Snowden have had for international security and inter-state relations.
Endnotes

BIBLIOGRAPHY

BOOKS


JOURNAL ARTICLES


Martin, Deborah G., Susan Hanson, and Danielle Fontaine. "What counts as Activism?" The Role of Individuals in Creating Change. *Women's Studies Quarterly* (2007).


**REPORTS**


INTERNET SOURCES


EZLN. “Today we say: ‘Enough is Enough’ (Ya Basta!)” http://struggle.ws/mexico/ezln/ezlnwa.html


Martin, Brian. “Activism, Social and Political”.


PC Tools. “What is a Computer Worm?”. *PC Tools.*

Reuters. “British Spy Chief warns Snowden data is a 'gift' for Terrorists”. *Reuters.*

Reynolds, Paul. “Eyewitness: *The Battle of Seattle*”. *BBC.*


**DISSERTATION**


VIDEOS


Discovery Channel, “The Secret History of Hacking” provides great insight into the genesis of mainstream hacking. See https://www.youtube.com/watch?v=Y47m1cOyKjA


PRESS RELEASES & STATEMENTS


